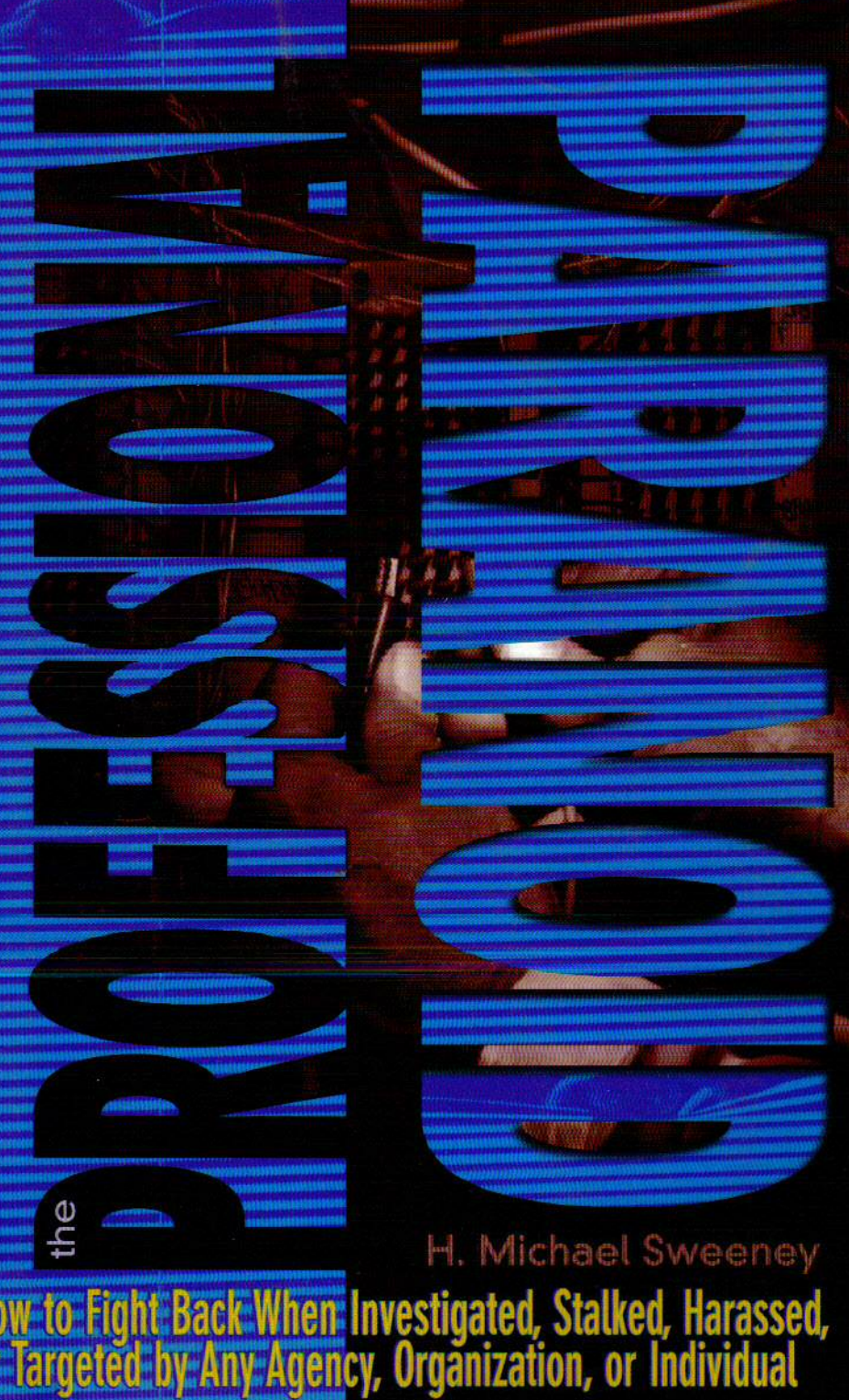
the
PROFESSIONAL
PLOT
H. Michael Sweeney
ow to Fight Back When Investigated, Stalked, Harassed,
Targeted by Any Agency, Organization, or Individual

THE Professional Paranoid

ISBN 0-922915-54-7

Design by Linda Hayashi

A Feral House Book
2532 Lincoln Blvd. Suite 359
Venice, CA 90291

www.feralhouse.com

10 9 8 7 6 5 4 3 2 1

THE Professional Paranoid

H. Michael Sweeney

FERAL HOUSE

ACKNOWLEDGEMENTS

This book, like the proverbial Phoenix, rose from the ashes of a troubled and stressful time. I dedicate it to the memory of Ace Hayes, a former intelligence operative who passed away recently after decades of fighting the same foes as I—his former employers. I learned a lot about my enemies from him. I think I showed Ace a thing or two he didn't know, as well. But we both paid a price.

What our common enemies did to us tore at the basic elements of our lives, making pawns out of anyone close to us. For that reason, I wish to thank my wife, Janet, for believing in me right from the start, for not joining with those who judged me as merely paranoid, and for being stronger than the unseen forces around us. Likewise, I thank my close friend, Dale, who never doubted for a moment, and who provided critical help. Not once did they ask me to prove my case—they just accepted my claims and offered their help, even when it cost them their time, effort, and money.

But others paid a price, too. My older daughters and my mother—all strong and unwilling to give in to the unique kind of terrorism inflicted upon our family—deserve special praise and thanks. In the latter days, several members of the intelligence community provided special help which earned my gratitude and put me in their debt. However, I cannot reveal their names here, or how they helped, so I will simply say thanks to you all. (Well, perhaps I will mention one, safely: Thanks, Terry, for standing guard hours on end in the cold of the winter night, and the rest.)

A special thanks to Adam Parfrey at Feral House, who sought me out at a time when I couldn't get any other publisher's attention, and who has a special sense of what is right and wrong in the world. Thanks also to Rick Weldon for his editorial wisdom and willingness to suffer under the gun of a deadline on my behalf. Thanks to James Atkinson at Granite Island and the original "debugman," Tim Johnson, for allowing me to steal so much good information on electronic surveillance and TSCM. Others who contributed to this book would include my opponents, who deserve many thanks for their predictability and for assuming that we citizens are too stupid to know what is going on in this country. A very special thanks to Jim Ameresco for complimenting me on my writing style and encouraging me to write a book in the first place. Aum A Estes.

—H. Michael Sweeney

The Professional *Paranoid*

INTRODUCTION

Do you frequently feel like you are being watched? Do you think you are sometimes being followed? Are there strange noises on the phone? Do objects at home or at work disappear or show up in other places, suggesting that someone has been rummaging through your things? As a result, are you starting to look over your shoulder, check the rearview mirror more frequently, show more caution with strangers? Does this make you a loony, a paranoiac? Perhaps that's what others already call you behind your back—or even suggest, to your face, that you might want to seek psychiatric help. Gee, they must be right—you must be crazy, huh?

After all, if you perceive a threat, it's likely that you act that way in the eyes of those around you. But it's a thin line between reality and paranoia, between someone who is truly paranoid and someone who is merely reacting properly to protect themselves. So don't take it too harshly when they use that nasty word against you. Instead, get some help. And here it is...

To begin with, take heart: even if you only think you might be targeted by some person, group, or agency, it is probably true, despite what others may think or say. There is a best-selling book by Gavin De Becker that will make an excellent companion to *The Professional Paranoid*. Called *The Gift of Fear*, it explains exactly why your instincts are your best tool in determining if you have a problem. The most important thing to realize is that the problem is not how others perceive you. It is not even so much that you have an enemy, as much as it is that you must acknowledge the threat may exist. Only then can you take appropriate action.

As De Becker would point out, when we perceive basic instinctual responses to events around us, all too often we simply choose to ignore them. That strange sensation of being followed or being watched is a natural instinct, and there is surely something in the real world that is causing the instinct to be triggered. The noises on your phone and the clues left in your drawers are real-world signals that your instincts are trying to point out. Yet all too often, we dismiss these impulses with all manner of disbelief, consciously struggling to accept a suspicious stranger or event as OK while insisting to ourselves, "Oh, it's nothing, I'm just being paranoid."

In today's world, men and women interact with many people in an extremely rich and complex way. Despite whatever care we may take in our interactions, there are lots of ways in which we might

make enemies of other people. Often, we don't even know when we cause people to feel slighted, insulted, or angered; we may feel a sense of awkwardness in a given situation, but we may not realize the extent of the damage. Sometimes we cannot be expected to know, for the damage may reside entirely in the head of a deranged individual. In your daily travels, you may unknowingly cut someone off on the highway, you might say or do something that someone else perceives as insult or threat. When they decide to make you their enemy and elect to go to war, they automatically become your enemy by default—though you may not even yet know it. Unless you have an opportunity to salve the perceived wound, the problem can grow to out of proportion and represent significant danger.

Often, your new enemy elects to secretly cross over the line of legality, morality, and, certainly, the civility we would like to think common in our so-called civilization. This often means that they don't play by the rules, and they start by being as sneaky and stealthy as possible. They don't usually send out a warning letter (or if they do, they do so anonymously). They just start their war against us in secret. For instance, that guy on the road drops back and follows you home, and then plots how to best take advantage of knowing where you live.

Thus, if it were not for your instincts, you might not know they were near, watching, making plans, plotting. Your instincts ... intuition ... gut feelings ... bad vibes ... are all your best defensive tool. Be more like the animal in the woods. Pay attention to your instincts. They might save you a good deal of trouble—they may even save your life.

Throughout *The Gift of Fear,* De Becker recounts the tales of people who, for reasons they could not understand at the time, simply felt something was wrong. Indeed it was in each case, and if they had not reacted appropriately in response to their instincts, they could have suffered great bodily harm. The clues were there but not in plain and focused view. Yet these people's minds absorbed the information and subconsciously processed it to put together a correct picture of potential danger. The subconscious has its ways of getting our attention, through intuition, vibes, and the like. But it won't just walk up and give you a peck on the cheek. Stop and think about it, whenever you get those warning signals. Something could be afoot. The root word from which intuition springs is tuere, which means "to guard or protect." The French word *tuer*

takes it a step further, "to kill." Hopefully, you won't have to go that far to defend yourself.

I can testify that intuition is a great defensive weapon. I was no different that you, most likely, when my first encounter with an unseen enemy came about. Wandering through my existence, I happily concerned myself with the minutiae of day-to-day tasks and goals. One day, while I was in the waiting room of an auto dealership's service center, reading a book on Watergate and hoping to hear that my car was ready, a man entered the room and sat in the seat opposite to me. I glanced at him, and, while the vibes were definitely not good, I let it go. There was no real cause for there to be anything seriously wrong, I thought.

After some time, I decided to call my wife on my cell phone, but I didn't want to do it in public. I rose and left the building, walking down a maze of hallways that led to an exit at the back parking lot, a lot used only by employees. After stepping outside, I produced the phone. Something told me I was being watched—a second instinctive warning. I maneuvered the phone in a way that brought it up high and allowed me to cock my head enough to glance at a window situated between me and the door I had just used. In the window, I saw the reflection of that very same man, standing there and peering through a small window in the door. He had followed me immediately after I had left the waiting room, all the way down two corridors to an exit for which he should have had no business. He just stood there and watched me the whole time. When I put the phone down, he vanished. I could not find him anywhere in the building, and no cars had been announced as being ready while I was outside.

In retrospect, I saw how my subconscious had warned me. What happened, of course, was that my instincts were put on edge by virtue of the fact that this man fit the description of some of the Watergate burglars—he looked Cuban. This was the source of my bad vibes—the Watergate burglars were CIA, and I was at the time researching illegal activities of the CIA. My brain simply clicked without my knowing it. Furthermore, I had subconsciously noted that he was always looking my way and even directly at me when I looked at him. When I left the room, I perceived a motion behind me, as if someone else was standing up. My mind put all this together and deduced that there was a strong possibility I was being followed. I listened to these strange warnings enough to at least glance at the window out of the corner of my eye. Yet even

as I did that, I'm not so certain that it was a conscious effort, though I remember thinking in an instant to deliberately move the phone to allow for it. The effort paid off. Instincts work. Trust them, and damn the consequences—don't fear being called a paranoid. That is a much better alternative than being caught off guard and attacked by an unseen opponent.

That was the start of my war with the intelligence community. I would end up going head to head with a number of intelligence agencies, law enforcement types, and even ex-cons and other civilian players over the next several years. They spied on me, but there were also attempts on my life and other attacks on my business and my family. My response was no different than if the CIA itself had become aware that the (now former) Soviets were spying on one of their offices: counterintelligence. I spied back, and I learned who my real enemies were, where they lived and worked, who they reported to, and why they feared me enough to call me enemy worthy of assault. That story may help you have confidence in my abilities to properly write this book.

How It All Began

My adventures in counterespionage began in early 1992. At the time, I was a consultant to inventors and other businesses seeking investment capital. One client, a friend of mine, showed me a document he had described in our previous conversations. Supposedly a historical account of crimes committed by various people and groups since 1947, it was, in my opinion, an extremely crude and poorly written work. Filled with claims left unproven, it seemed flawed, obviously biased, and written in a cowardly, unauthoritative manner, with no bibliography or author information given.

However, as I went through the document, a couple of things astonished me. It viably tied certain people associated with the assassination of John F. Kennedy to the Watergate scandal, providing specific information linking the two. It was much more detailed than any other similar report I'd ever read. In other published accounts I've seen, the connections had been always been addressed in sweeping, generic descriptions or had never been mentioned at all. If these claims were true, the document was not only important, it was a potential powder keg. I wrote to a former intelligence agent in a position to assess its accuracy. My

contact was an author on politics and happened to owe his publisher one more book under the terms of his contract. If anyone could do the subject justice, I reasoned, it would be him. And unless he invited me to be a co-author, I felt no reason to be further involved.

Within three days of my inquiry, my life began to fall apart. It became clear that I was being followed, and I took precautions which enabled me to detect several surreptitious entries into my home. While I was away, my computer was tampered with, sabotaged, and eventually stolen. My mail was intercepted and my life put under electronic and visual surveillance at both work and home. In one incident, I was victimized by police who responded to a 911 call I made concerning prowlers on my property. Though numerous witnesses confirmed that I had chased away two people (with a toy gun, no less), the officer filed a report that mentioned nothing other than that I was mental.

Furthermore, my business was derailed by a number of means, including the sabotage of my relationships with federal agencies operating in American embassies abroad. (In my job as a consultant, I often dealt with potential investors in foreign countries, who would invest in American businesses in exchange for American citizenship under the Immigration Act of 1990.) I was eventually forced into bankruptcy. Relationships with friends and family were also affected adversely by the emotional stress of the situation.

Despite all of this, I fought fairly well against my antagonists. I was able to turn the tables on them, to follow and identify them, find where they lived, where they worked, who their associates were, and so on. I found ties to CIA fronts and even to Langley, Virginia, itself. I succeeded partially due my alignment with a rather loosely organized underground of individuals active in their opposition to governmental abuse of power. I met and befriended a surprisingly large number of people nationwide who had personal experiences similar to mine. Through insight gained by their successes and failures, I was able to learn the "trade."

The goal of this work is to help the inexperienced to deal with forces intent on the invasion of your privacy, regardless of whether it's the FBI, CIA, IRS, or just some idiot bent on causing you trouble. In presenting this material, no presumption of prior knowledge is made on the reader. For that reason, some content may seem all too obvious or basic to many readers. But given that so

many people who have come to this author for help have no experience upon which to build, I will start with the basics to ensure that everyone can comprehend.

Rules For The Paranoid

There is only one hard and fast rule ... that there are no rules you cannot break or bend to your needs. But the following may serve you well in a tight situation. Always be on the lookout for anything unusual. This can be anything from a car passing by repeatedly to changes to your own car. It might be a door left ajar that you know should be closed. Obviously, you must regard what others may do in your absence. Establish rules of procedure within your household or place of business, and be thorough before drawing conclusions.

Document everything. Note dates, times, license plate numbers, witnesses, details, and your own thoughts at the time. Keep track of who, where, when, what, and how. Keep a journal, and photocopy any evidence you uncover, take statements from witnesses, etc. Keep originals in a very safe place, such as a safe deposit box. Use of tape recorders, cameras, and camcorders can be very valuable. Install security cameras if the need arises. Be able to produce a camera or recorder at any given time. Consult a lawyer and ask about laws in your state regarding surreptitious recording.

Be flexible and quick. Have a contingency plan and be ready to go on a moment's notice. Have more than one route to work. Take a change of clothes for disguise with you or have sets of such clothing at your place of work, your church, etc.

Be unpredictable. Establish patterns and then break them.

Set indicators and booby traps. You can do a variety of things to alert you to breaking and entering or tampering. Devise tests which may reveal your enemy's actions or intentions. Bait them into taking actions beneficial to you (so you may catch them red-handed, with witnesses or on video, for instance).

Don't put your trust in official resources. Look for ways to ensure the loyalty of professionals you must rely on but have no basis for absolute trust. If you must contact the police, talk to several people in different departments and let them know you are doing so. This will help keep them in check.

Remember that your opponents are human and will have

human emotions and frailties. They are subject to human error just as you are.

Make allies out of strangers. I've gotten people to provide confidential information and obtained covert aid and funding. Don't underestimate kindness.

Be direct. Don't be afraid to walk into your enemy's camp and confront them if you feel it's appropriate. You may decide that it's best to discuss the matter openly. You never know what you might uncover. You may even be able to resolve your dispute then and there.

Be unreasonable when the situation calls for it, and don't be afraid to make a fool of yourself. Go ahead and stare, run a red light, be rude, cut in front of someone in line, start an argument.

Let secrets out. If your enemy is watching you, feed them information from time to time that keeps them feeling successful. Choose older and less-harmful information, and don't just hand it to them: make them ferret it out.

Don't assume any person, thing, or event is what it seems to be. Be suspicious, and verify everything. Keep your wits about you at all times.

IDENTIFYING THE ENEMY

The first step is to determine who your opponent is so that you may tailor your strategy and respond accordingly. In this segment, I'll discuss what is unique about each "bad guy" and what makes them different from or similar to each other. This may help you determine the scope of your problem. Even if you think you already know the answer, reading each of the following sections may help you define the nature of your antagonist. You may even find that you have more than one enemy allied against you.

Knowing precisely who your enemy is can be valuable for other reasons. If you know who your enemy is, you will gain not only insight as to why you are targeted but you will also have an opportunity to predict what lies ahead. If you know both who and why, you can likely deduce their goal and predict how they might reasonably expect to meet that goal. Knowing who they are and what they want will also likely tell you a lot about methods. As a precaution, however, I urge you to consider your enemy in much the same way as a military planner—don't make plans on what an enemy might be expected to do, but rather, make plans according to their capabilities. That is, make contingencies based on any action they might be able to undertake, regardless of how illogical an action might seem. Cover all the bases you can, putting perhaps more energy and care into those you find more reasonable and likely.

Can you accurately predict an enemy? To a degree, yes. I quote from *The Gift of Fear*: "The truth is that every thought is preceded by a perception, every impulse is preceded by a thought, every action is preceded by an impulse, and man is not so private a being that his behavior is unseen, his patterns undetectable. Life's high-stakes questions can be answered: Will a person I am worried about try to harm me? Will the employee I must fire react violently? How should I handle the person who refuses to let go? What is the best way to respond to threats? What are the dangers posed by strangers? How can I know that a babysitter won't turn out to be someone who will harm my child? How can I know whether some friend of my child might be dangerous? Is my own child displaying the warning signs of future violence? Finally, how can I help my loved ones be safer?"

To begin with, if your instincts prompt you to ask these kinds of questions, it is a warning sign that you had better carefully examine every aspect about the situation. Start by asking yourself just what

makes you nervous enough to ask the question. What are the warning signs that triggered your instincts? The temptation will be to dismiss or deny the significance, but for the sake of evaluation, do not allow dismissal of the issue. Keep digging. If you find multiple signals or reasons exist, you likely have a genuine and significant threat. This will help you identify an enemy when it counts—before they attack. It will also help you calculate their next move because their motives and means will become more clear.

Stalkers and Personal Enemies

Old lovers ... business associates ... stalkers ... neighbors with an ax to grind ... whoever they may be, private citizens are perhaps the easiest to identify, for they are more likely to be obvious in their actions and intent. Generally motivated by emotion rather than logic, they tend to be somewhat haphazard and spontaneous, prone to mistakes, which, depending on their misstep, can be good or bad for you. The one dangerous exception to the emotion-versus-logic rule is the psychopath, who can be so clever and careful that you will have to be equally clever to trick him into erring. Generally speaking, however, harassment by private citizens is the least of your concerns.

Your problems with these types will likely fall into the nuisance or prank category. They typically seek to find ways to anger you or cost you money (usually the same thing). Unfortunately, unless you nip it in the bud, your problem can grow—all too frequently into felonious actions such as arson, assault, kidnapping, even murder. But how can you deter someone before their harassment escalates? Only by making them believe that an offensive action will result in more harm to them than to you. You must stop them cold by putting them in a position where they face the threat of landing in jail, being fired, losing valued personal relationships, and so on. Notice I did *not* say that you should actually harm them with these actions—it is simply the ability to do so that you seek. This requires that you gather actual evidence or resources which you can use against them.

With this, you can not only hold a significant threat over them but act on the threat, if necessary. If you hold some sort of damning evidence against your foe, for instance, you might secure a restraining order or file civil or criminal charges. A lawsuit can attach a financial penalty which not only compensates you but also provides contingency rulings for superlative restitution. The best

scenario might be to sue, then settle out of court with stipulations in your favor. Your bargaining chips can include the reduction of financial or other penalties, dropping of any criminal charges, or concessions regarding your original dispute. Just be certain that the penalties for violating any of the terms are extremely harsh. Of course, it would do no good to hold over someone the threat of, say, forfeiting a huge sum of money if they have none. It must be something they have but do not want to lose.

Checklist For Stalker Victims

- ❑ Avoid daily routine or patterns in your travels and habits. Don't let the stalker be one jump ahead of you.
- ❑ Learn to detect being followed and to evade attackers, and arrange for escorts.
- ❑ Be aware of your surroundings and others at all times.
- ❑ Act confident.
- ❑ Always keep an eye out for possible escape routes or places to seek help.
- ❑ Arrange for changes of clothing, wigs, or disguises to be available at work or other destinations so you can make a clean getaway if need be.
- ❑ Keep a change of clothes in your car.
- ❑ Consider purchasing a cheap junker car to be left at a destination of your choice, to allow for a quick undetected change of vehicles.
- ❑ Be prepared to vanish on short notice. Always have credit cards or cash ready so you can immediately check into a hotel/motel if you need to. Don't go to your ultimate destination unless certain you are unobserved. Keep an overnight bag in your car.
- ❑ Always notify others when to expect you.
- ❑ Involve the authorities and legal help each and every instance. File complaints, charges, or lawsuits, or file for injunctions or restraining orders where possible. Document everything, and have witnesses. Once it is official, slander is less of a worry.
- ❑ Learn self-defense, consider weapons for self-defense, and be willing to use them. Second thoughts, fear, or doubt can kill you. As a general rule, it is legal to defend yourself by any means necessary, if you fear for your life. Check with your local law enforcement.
- ❑ Strengthen the security of your home, workplace, and vehicles.

- ❑ In any encounter with a stalker, attempt to get to a crowded or public place. Make a scene and draw witnesses. Point to the stalker and accuse. Get witness contact information, even if the stalker did nothing suspicious—you need to illustrate the stalker's frequency of attention.
- ❑ Attempt to fully identify and understand the motivation and habits of the stalker. Attempt to predict their behavior and plan for any possibility.
- ❑ Consult the police *and* a private detective.
- ❑ Don't destroy or throw away any items that come from the stalker. These can be used as evidence.
- ❑ Don't allow the stalker to control your emotions and actions. They generally want you to be afraid and will see any curtailment of your lifestyle as a sign they have succeeded.

Women Can Be Paranoid, Too

Recently, I asked a number of women I knew to discuss their experience with stalking, assault, or rape. To my horror, every single woman I asked, including my wife, could speak of at least one instance in recent weeks. So how can we minimize the chances of danger? What are these warning signs? Let's start with the behavior of a would-be stalker/rapist/attacker. Anyone intent on such evil is going to put on a false face. They will attempt to deceive. Everything they say and do will likely be a lie, but they will be so charming and friendly that overabundant charm itself should be a warning. There are significant clues available within the patter of their seemingly natural conversations. In many cases, these clues are part and parcel of a progression of events which are necessary for most attackers to make good on their plans. They can be recognized by the would-be victim who knows how to look for them.

Basically, the attacker wants to:

1. Make contact: find an excuse to get close enough for conversation.
2. Lower defenses: Be friendly and charming. Have the conversation mapped out and take control of it.
3. Obligate and gain trust: endear yourself to the victim. Do some favor or task which indebts the victim, preferably one which is an ongoing task and allows you to accompany them to a more private place.

4. Isolate: Using the trust gained, isolate the victim from others. Be prepared to counter objections at the last moment.
5. Attack.
6. Cover up: destroy all evidence, including the victim, if necessary.
7. Escape: make your exit without being seen.

To accomplish these seven steps, the stalker/rapist/attacker will generally have everything planned out to the last detail. So another warning sign would be timing, that the event in question occurs when you are vulnerable to a possible attack. It is one thing for someone to approach you with an offer to carry your bags from the Main St. store front to a waiting taxi in the middle of rush hour, and an entirely different matter for them to offer to do it from your car in your driveway to the side door of your house late at night with no one else about.

But there are other clues, such as what De Becker calls Forced Teaming. The assailant tries to find a way to imply that you and he have something in common. He might say something in an offhand way about goals you might share or things you both do—peas in a pod. He tries to imply an artificial closeness or tie which is intended to cause you to drop your guard. "We did that pretty will, didn't we? We can't let that happen. We should ask ourselves what we could do about that." Forced teaming rarely comes about in conversations unless there is a genuine relationship already established.

As mentioned earlier, an overabundance of charm is another clue. People are not normally genuinely charming and nice to strangers, smiling broadly and warmly in general conversation. Polite is acceptable. But anyone who goes out of their way and who becomes very talkative and overly friendly is probably trying to convince you of something. How does a salesperson act when you go into a retail store where the employees are paid on commission? They go out of their way to be friendly and talkative. They smile as much as they talk. I know, because I sell computers when I'm not chasing spies. We are trying to convince you of something when you enter our lair.

Another clue is too many details. People who are trying to convince you of something will volunteer too many details. The purpose of the extra information is to provide additional evidence that what they say is genuine. If it were genuine, there would be no need

for additional evidence. An honest person might say, "I live across the street and saw you coming home from my window. I thought I'd introduce myself." A would-be attacker, however, would say something like, "I live across the street with my mother. She's ill. Parkinson's Disease. All she does is watch TV. I don't like TV very much, myself. Burned out on it when I was a security guard and all I did all day was watch TV. So, anyway, I spend a lot of time watching out the window. That's where I saw you coming home the other day, wearing the pretty blue dress. Anyway, I thought, 'there's a very pretty young woman I'd like to meet.' Something about your face..." The details in the story are designed to instill trust. A nice man would take care of his ill mother. You should feel sorry for him and for her because of the illness. He used to be a trusted security guard. He compliments your clothes and appearance. All that extra information is a warning clue.

Then there's Typecasting, a bit of reverse psychology. The would-be assailant seeks to manipulate you by typecasting you as someone who would never do certain things, trying to lead you into doing them. "Oh, you're probably too proper to go to a movie with a perfect stranger." Or, "I can't tell you that. You wouldn't understand me. Most people don't understand me." Again, these kinds of statements rarely evolve in normal conversation. They should alert you to try to find where the conversation is going.

My personal favorite, though, is Loan Sharking. The villain will create small, fictitious debts designed as a foundation so that he can pressure you to "return the favor" later on. You drop something, he picks it up. He pulls you back from the curb's edge to prevent you from being splashed by a car. He doesn't offer to help load your trunk with groceries, he just loads. Yes, nice people might do these same things, but unfortunately, in this day and age, you must always be wary and look for a motive.

If you begin to find more and more clues that you may be in peril, you should be thinking ahead to where he wants the encounter to lead and about your own evasive and self-defense tactics. There are some simple steps you can take that can help and that directly counter his strategies against you:

1. Disengage the conversation. Coldly, flatly, and firmly.
2. Draw attention: Call for help. Drop everything and flee for help

3. Defend yourself: Fight back to the best of your ability.
4. Collect evidence: Note details about his face, clothing, and identifying marks.
5. Thwart escape: Try to get witnesses. Get his license plate number.

Avoiding Assault With Dates

In all things, trust your instincts. Remember, too, that alcohol and drugs dull your senses and put you at risk—they kill your instincts. Here's a quick checklist to help avoid the situation altogether.

1. Check out prospective dates beforehand. Check with others who know the person. Don't be afraid to cancel the date.
2. Let others know what you are doing, where you are going, and when you will return, and let your date know.
3. Be alert to your surroundings and the progression of events. Look for warning signs. These are especially important for first-date situations.
4. Make your romantic limitations clear from the outset of the date.
5. Be prepared to terminate the date—have money for transportation and a cell phone, if you won't be near a pay phone.
6. Be careful when considering inviting a date into your home or accepting an invitation to the date's home.

Avoiding Assault in General

The following are all common sense, but sadly, most rapes happen just because one or more of these common sense rules were ignored.

1. Keep doors locked, use peepholes to identify anyone at the door before opening it.
2. Keep windows and drapes closed at night.
3. Use timers on lights and radio/TVs when away, keep your car in the garage when at home. Require identification from strangers seeking admittance to your home.

4. Don't let strangers in to use your phone—call on their behalf while they wait outside.
5. Don't use your full name in telephone books or mailboxes—use initials.
6. Avoid wearing name tags with your full name at work—use a nickname or first name only.
7. Do not wear such badges outside of work.
8. When approaching your home or car, have your key ready or use a remote to unlock.
9. Never enter a home or any building where it is apparent that someone has gained entry without permission. Call 911 immediately. If in your home or any location where forced entry is being made, call 911 and stay on the line. Do not leave the building unless instructed to do so.
10. If you jog or go for walks, always oppose traffic. Try to go with someone else you know, or consider a large, noisy dog for companionship. Avoid using headphones, as they blind your senses so that anyone can come up behind you without your hearing.
11. Consider an alarm system for your home.
12. Take self defense courses.
13. Never stop for or pick up strangers.

Private Detectives

Private detectives pose an interesting problem, for they run the gamut of skill and ability from borderline amateurs, clumsy as bulls, to very sophisticated professionals with considerable experience and resources. It might be someone doing it for fun, with only a mail order detective's course as his guide, or he might be a retired FBI agent, with friends in the "business" willing to do him favors. I've been dogged by gumshoes of that ilk at least once, during my investigation of the Flight 800 tragedy for a book entitled *Truth In Flames*. Ironically, I am applying for a P.I.'s license myself in order to enhance my investigative writing capacity, and I'll be joining associations where my "opponents" will become my peers.

Normally, even the worst detective will operate within certain ethical guidelines, which can be to your advantage. Unfortunately, it is possible to find one who is willing to go over the line. This, too, can work for you. In order to benefit and be safe, however,

you must take care to determine which you face. Some states will provide you with a copy of ethics guidelines and rules for P.I.s, and knowing these will allow you to act more freely—as you can evaluate their likely response to a particular strategy.

If your opponent is ethical, you can depend on him to follow some fairly well-defined operational procedures and limitations; for instance, you need not be as cautious in secreting information if you know that unlawful entry is not an option to the detective. If you have determined that he will operate outside of the law, you can bait a trap which, with photographic or witnessed proof of legal transgression, will net you leverage. Either way, you typically can rely on a private detective to follow some fairly narrow rules of operation.

Most P.I.s try to work within the law, stretching and bending, rather than breaking it. They will seldom enter a residence illegally or tap a phone line because these steps can easily land them in jail and out of business for good. They generally work in a methodical, almost robotic, fashion on assignments which tend to be fairly specific, making them predictable and, thus, vulnerable.

Say they are told to dig up dirt on you. In such a case, they will be everywhere, looking into everything. Check with your credit agency to see who has recently inquired. See if anyone has called your office with questions about your schedule without asking to speak to you. Speak with everyone you are close to personally or professionally to find if anyone has made inquiries or comments that might raise a flag. Take notes and get descriptions.

On the other hand, they might have simply been told to follow you and keep track of where you go and who you see. Usually, this means that they will be desperate not to lose you and will run a red light or speed to keep within a reasonable distance of your car. Often, their assignment is given such an urgency that even when caught "in the act," they will still try to stick with you. That is a rare but undeniable opportunity to establish witnesses or other proofs in your favor, identify the person, or even confront them.

There is no particular danger in confronting a private eye, even though they may present an aggressive front. You can generally engage them in reasoned and useful dialog if you enter into the conversation without being overly angry or violent yourself (and don't even think about a using a gun or strong-arm tactics). Should you think it wise to confront them, have a game plan and know

exactly what you plan on saying. Be prepared for unpleasant and unexpected questions. While you are not obligated to answer any question, you also don't want to reveal which are sensitive in nature by an unprepared reaction. An innocent, blank expression is better than a look of horror.

Tell him you know what he and his client are up to. Give evidence to let him know you aren't bluffing—and don't bluff unless you have a pretty good idea it'll fly. Generic is good, specific is foolhardy. Advise him that your lawyer is ready to proceed in a civil or criminal suit against both of them, and imply that you're willing to negotiate with his client to reach a settlement. Consult a lawyer first to be sure that you the option and are willing to act on it—in some cases, an empty threat of litigation can itself be grounds for a suit.

In addition to this confrontation scenario, you have several other avenues to pursue once you have identified a detective. Keep in mind that he is not your enemy, *per se*. Your true opponent is his client; the detective is merely a tool. Your most important goal may not be to thwart the detective in his job, but to learn who he works for and what his assignment is. Countersurveil to find out who visits the office, or follow the detective to find out who he reports to. If you can identify his client, send an unsigned note or make a phone call to say, "I had a little chat with your detective." Hint that the detective was cooperative. This simple act could sabotage their relationship—but good. Of course, in this case you'll likely want to watch your opponent to see who his next detective is...

One final note regarding detectives. Several of the larger national detective agencies and many of the smaller, local ones, are, or were at one time, CIA fronts. Regardless, they may have a high percentage of "retired" CIA types in their ranks. If your detective comes from Wackenhut, one of the better-known firms founded and staffed by former intelligence officers, then you may have a bigger problem than you had originally anticipated. Also, keep in mind that larger agencies have resources which will outstrip those of your typical one-man operation. Still, balance this thought with the fact that there is no action unless the client is willing and able to pay for costly additional resources.

Corporate Bullies

These are generally corporate security guards which might be used against you as part of a "troubleshooting" operation. If you have crossed a major corporation, you may have gained the attention of such a group. Despite the notion that a corporation is part of the community in which it operates, it's a sad fact that, often, the larger a corporation is and the more money they stand to lose in a given situation, the less attention they pay to their public image or the law.

A corporate security force is generally headed by someone who is results oriented and who operates under the notion that the end justifies the means. Within his force, he tends to employ or retain a small handful of "experts" in various illegal fields who can be called into play when needed. Like private detectives, these players tend to have a narrow focus and limited flexibility in regard to their duties. This will make them easier to spot, identify, and deal with than some other opponents. Keep in mind that, to them, it's just business, and you can use this fact to your advantage. In some cases, though, they may be seeking to protect a secret you have no knowledge of, and this can foster miscalculations. You have to be careful and avoid sweeping assumptions.

Gangs and Petty Criminals

Street gangs can pose many problems, as they act to perpetuate themselves in a number of ways by gaining turf, money, notoriety, and so on. Some are highly organized, some are completely unpredictable, but all are tenacious once they grip a community. Many of a gang's more violent or criminal acts are related to internal struggles or have to do with rival factions. When violence spills into the community, innocents can suffer as well, but there are some ways in which gangs go out of their way to affect outsiders who reside in or do business on "their turf." If you find yourself victim of gang violence or crime, your position can rapidly become very precarious.

For this reason, a special disclaimer is required. You should, by all means, consider law enforcement your best ally, unless it becomes clear they are unable or unwilling to provide adequate assistance. Any actions you undertake on your own, including those suggested here, should be considered with the utmost care with respect to personal safety. Nothing suggested here should be

undertaken without first exhausting all other alternatives, and if you decide to take defensive action, you do so at your own risk.

One common way gangs prey on the community is the practice of the classic extortion method called "protection," in which payments are required to defer damage to you or your property. If you are threatened at your place of business with a protection racket, simply record their threats on audio or videotape. Should they choose to speak in couched words which might be construed as less than threatening, defy them just enough to cause them to react with sterner warnings. Their action against your business will generally follow a simple, predictable pattern of escalation. Politely delivered but suggestively disturbing threats are followed by aggressively delivered abusive threats. Next comes shouting and curses, perhaps accompanied by physical action but usually limited to token damage of property. In the end, you, your employees, or even your family could suffer serious damage to property or physical assault.

Escalation works two ways, however; it gives you the advantage of choosing to resist early on—something they might naturally expect anyway. You can then force them to escalate and catch it surreptitiously on videotape. The next time they approach, you can "give in" and pay them off—also on tape. But this is not enough. Generally, the gangs know that the cops might be called, and so they deliberately try to avoid association of personal actions to gang activities. If caught, the ones threatening and collecting go to jail, and the gang at large remains free. Part of their threat is that you can't get them all, and they can easily get even with you if one of them is caught.

Therefore, you must have help. I advise you to hire a private detective because a gang may be too dangerous for friends or relatives to risk involvement. The detective can surveil the outside of your store or home, waiting to photograph or videotape the proceedings in an appropriately covert and undetected manner. When one of them enters, give a signal. Make an effort to capture everything they do—including where they go next—on film or tape. They may hit another business, and in all likelihood, a different individual might then be the collection man. If you are fortunate, you may be in a position to demonstrate that each of the members is involved and perhaps even press charges against them all.

That, however, may still not be wise, as gang affiliations can be very strong and widespread. One method that might work is to zero in on the gang's leader. Show but do not give him a copy of

the tape. Stop the tape before he can see it all, implying there is more on the tape than there may actually be—keep him guessing on his exposure and risk. Inform him that you have a relative on the police force and that the game plan, if anything happens to you or yours, is that HE is the one to go to jail—first. Tell him that the cops will wait a short while and then pick up the remainder, who will be informed that they have been ratted on—by him. That should plant an unpleasant notion in his mind. Suggest that the only alternative is to drop his interest in you. Suggest that he will ALSO want to protect you from rival gangs—after all, how could you be expected to know which gang is troubling you?

Of course, in the final analysis, it may be safer just to pay what they demand or to shut down and move on. Only you can decide where to draw the line and how to react if crossed. It is your neighborhood, your place of business, your family, and, therefore, your decision.

There is also the issue of gang graffiti. It should never be allowed to accrue or stand long anywhere in your neighborhood. Work with the police and city officials to arrange public work groups to repaint on a frequent basis. Working in numbers is the safest bet, especially with police assistance. If you really want to do an effective job of combating the gangs, learn to read the graffiti. You will be surprised at what it can tell you. Again, the police can help you in this effort and will be thankful for the tips you can throw their way by that ability.

Professional Criminal Elements

The issue of crime syndicates is a tougher one. If these guys are angry with you, there's usually it's because you've given them a reason. These folks are almost always direct and up front, so at least you'll be aware of the exact nature of your problem. But they are nasty and will let you know it. Like petty gangs, you will first want to use police as your first line of defense, and unless they are unwilling or unable to provide the needed assistance, do not undertake a confrontation unless it is your only remaining option. The professional criminal can be very dangerous and should not be taken as a lightweight threat.

Your options may well be the same as with a gang, though you may need some kind of "insurance" other than a videotape. The people you are likely to be able to catch on tape are probably too

low on the totem pole to be considered valuable by their boss. Still, if you get the right opportunity, you might be able to use such a tape to pressure a lower hireling into cooperating somehow—enabling you to get the needed information on the big cheese himself. Your best allies will likely be law enforcement at either the local or federal level. Be careful, though: the cops are often in tow behind the criminal kingpin.

The Law

Local cops can be quite manageable. If they're on your case, you are either a valid suspect in a legitimate investigation or, conceivably, the subject of political, racial, or personal harassment. It is conceivable that you may be under legitimate investigation and also being harassed. In any harassment case, your lawyer can safely exercise your "insurance policy" for you. Do not attempt it yourself unless you have witnesses and are extremely careful about what you say and how you say it—it can easily backfire and be used against you as if it were a blackmail or bribery attempt.

If under investigation, you will need to know why so you can work to prove yourself innocent or better trap those who harass you. Confront the police immediately with each piece of information you obtain, preferably through a lawyer. Where possible, get documentation (originals, not photocopies, unless notarized or accompanied by other proofs of authenticity), and keep it safe. Don't turn documents over to the police, just give them the facts regarding their existence and let them research their own copies. If you must provide documentation, do not give them originals. Note: There may be some instances where the nature of the documentation is such that you might be better off simply alluding to its existence—to avoid loss of originals by warrant or subpoena. Keep the originals safe at all costs for possible court use.

If you are being harassed by the police, treat it as a personal issue between you and those officers involved rather than you against the department, and again, get it on tape. This should be easier than with your other foes because cops will likely be conducting their harassment in the open, their confidence bolstered by their authority over you. Also to your advantage is the fact that they value their career and standing too much to endanger their future on the force. In negotiating with crooked police, you must take care to allow them a reasonable "escape" solution, for if you

have them backed into a corner, they might feel their only option is to take you out permanently.

State cops and county sheriffs essentially fall under the same guidelines as local cops. However, if you determine that the source of your problem is from these higher agencies, then consider the issue of jurisdiction—especially if you are unsure of why you are being investigated. These agencies have limited jurisdiction will not likely act outside of their territory—with a thorough knowledge, you will be able to better analyze your situation.

If you determine no jurisdiction, such as from a county or state where you have had no involvement whatsoever, then it is likely that someone at a high level is using their authority within the agency to harass you. Treat this the same as with harassment by local cops. If you determine just jurisdiction, then you may limit speculation regarding their involvement to those areas with which they have jurisdiction. For instance, a state cop does not normally investigate a capital crime that falls under county or city police jurisdiction.

Federal Cops include any of the following: FBI (Federal Bureau of Investigation, DEA (Drug Enforcement Agency), BATF (Bureau of Alcohol, Tobacco, and Firearms, also known as the ATF), and others too numerous to mention. Nowadays, it is also possible to run into a special Multi Jurisdiction Task Force (MJTF) operation. Despite the obvious issue of constitutionality, this can of worms can even include National Guard or other types of military agency cooperation, including the DIA (Defense Intelligence Agency).

You will want to determine which agency and what drives their interest. Generally speaking, the FBI doesn't care about drugs or illegal firearms, and the DEA could care less about a bank robbery suspect. But if one agency investigates you and in the process discovers evidence of illegal activity outside of their interests, they may actually prefer to keep it to themselves for a period of time so as not to risk interagency jealousy, which could cause damage to their investigation. If this happens, you could be at an advantage.

You may have few clues as to the agency. The FBI is discreet in inquiries and hard to detect unless you can find someone willing to talk. An investigation by the DEA, which relies heavily on informants, may suggest that there is someone outside the agency who has betrayed you to them. The BATF usually goes undercover and waits quietly for mistakes or other opportunities or, again, relies upon informants.

With respect to surveillance, these folks have almost unlimited resources and tend to use lots of vehicles and personnel. They often like to appear as utility-company employees or corporate entities. A single car following you is probably not a federal cop. Rather, look for larger vehicles, especially ominous-looking black vans with special aerial antennas or people who frequently hold mics or phones to their faces. When using multiple-car tails (tag teams), they may also have a mobile command post disguised as some sort of business or utility van.

Radio messages of current location and direction are relayed to the van, where a detailed map is used to route all vehicles to the next logical intercept point. At any moment, you will likely have one or more on your tail, and one or more in front of, and to each side of you. Double back frequently to try to locate any such secondary vehicles and perhaps even the mobile command post. Park in a position with good view of all access points and roadways, but blocked from distant view, and see who drives by—often more than once. I've seen a "plumber's truck" drive by seven times in one sitting.

Their job is to anticipate having a car near you at a moments and to swap closer vehicles frequently. If they really want you, they can attach a unit which tracks you electronically, permitting them to remain far back and perhaps even well out of sight. Once you stop and park, a surveillance team is set up to watch your vehicle, and a foot team may be deployed to keep up with you on foot.

The IRS generally gets right in your face up front. Watch out,for any such face-to-face confrontation regardless of how gentle or innocent seeming, can lead to sudden, unexpected interventions harmful to your financial well-being. If they are digging, they tend to assume you are guilty until proven innocent. They operate under laws they have written, which defy the bill of rights in almost every respect and are enforced by a separate judicial system they own and operate. They tend to abuse their power, to act first and let you ask questions later. They can freeze or seize your assets.

Thus, if you have any strange activity suggesting unwanted IRS interest in your affairs, you should take the following precautionary actions: Empty your accounts. Consult both your lawyer and a tax attorney about signing over all assets and property to a third person or establishing a trust or holding company. Consider an arrangement whereby you sell property to a trusted partner on terms while simultaneously leasing it back from them with an open-ended and favorable purchase option. The payments each way neutralize each

other—but must be exchanged. Establish safety provisions in case you are forced to suspend payments so that default does not cause loss of control over the property. The IRS cannot seize what you don't own, and cannot freeze what isn't in a bank.

Intelligence Apparat

The intelligence community is the hardest nut to crack. There are endless agencies: the CIA, DIA, NSA (National Security Agency), the FBI, NRO (National Reconnaissance Office), and separate intelligence operations under each branch of the military, including Department of Defense (DOD) and others. Fortunately, there is some good news. The FBI has narrow range of interests, as discussed before, and unless you are a spy, you won't have problems with the NSA, DIA, or the military.

The CIA, however, often seem determined to be involved in everyone's business, regardless of legality. The fact is, of course, that Langley (home to the CIA's headquarters in Virginia) would never directly do something that had a chance of giving them a black eye. This means the CIA will **never** be caught meddling in your affairs. The trouble is, they don't have to do it themselves. They have others do it for them, though of not officially. Any CIA spy work aimed your way will likely involve the myriad network of CIA "proprietaries," or fronts—and there are literally hundreds of these documented as operating illegally within U.S. borders, representing a mere fraction of the total, according to former CIA agents.

A proprietary is an otherwise perfectly legitimate private or public business. As such, it conducts (or at least seems to conduct) perfectly normal business in its chosen field. However, it also conducts covert (and illegal) CIA business. This "company" business is supposed to be limited to foreign intelligence or counterintelligence operations. But all too often, it is used to investigate or harass citizens, organizations, or companies in the private sector.

The chief difference between this type of operation and any others described thus far is that a CIA front operates without concern for cost, and escalations in spending are indicative of federal interest in your affairs. They have unlimited resources, and while they may start with a simple, one-man surveillance operation, they will happily escalate to any level of sophistication deemed necessary. They would think nothing of throwing dozens of people and vehicles into an operation, planting a dozen $80,000 bugs, buying

or leasing property nearby, or other equally expensive contingencies. Once, when I had been the subject of CIA surveillance for over a year, I estimated they were spending $250,000 a month on me. It's your money, why should they care?

Thus your initial contact with these operations might seem to originate from a private detective or cop. The only way to tell is to burn them, (i.e., let them know that you know they are there). They will advance to a more sophisticated technique—as described under surveillance techniques elsewhere. Any such escalation is your first significant clue. The nature of your circumstance and any likely match to their natural areas of interest are your other clues. If you are lucky, you can find ways to confirm your hunches.

During the time I was surveilled, I obtained information on a license plate which was determined to be blocked out of Langley. That is, the Department of Motor Vehicles had been instructed to say there was no such license plate. In many states, anyone can go down to a DMV office and run a plate. Only government vehicles can have blocked plates. Normally, I would only have been told only that the plate did not exist, but I managed to access a DMV terminal and see not only that it did exist but that is was blocked and by whom. If you live in a state where this is now allowed, unless you know a cop who will do you a favor, you can't use this tool—and you are at the mercy of your oppressors. The thing to remember about running a plate is if it's blocked and you have no additional way of accessing the information, not only will you gain no knowledge about the owner, but the supervisor of the agency involved will be notified of your inquiry. The other side will know you inquired. For that reason, you might consider finding a way to inquire under a name not easily associated with you, such as getting a friend to have his friend accomplish it for you.

Further, I was able to conduct good countersurveillance. I was able follow, photograph, and identify several of my foes, follow THEM and find out where THEY worked and lived. Investigating one company I had linked them to revealed a long list of irregularities, listed here briefly, all of which suggested that the company was, in fact, a CIA front. Any front you might encounter may or may not exhibit similar characteristics:

1. Doing business under seventeen names (very few of which were "visible" names to the public).

2. Different company names used on trucks and buildings. Similarly, different business names used for registration with the State Corporation Commissioner, County Tax Assessor, and City Business License Bureau—thus no agency knew of the other names, making it almost impossible to track them down through a given agency.
3. Though advertised as largest of its kind, it had no Yellow Pages listing. After searching for the business by its address, I found yet another name. This name changed from year to year.
4. Company trucks had no addresses or phone numbers on them.
5. The company was owned by a law firm with offices in Washington D.C. (fifteen minutes from Langley).
6. Tax records in two different counties each showed properties with addresses which did not exist.
7. Corporation Commissioner documents reveal significant irregularities in finances, which would appear to suggest illegal silent partners and millions of dollars in hidden funding.
8. Incorporation documents had whole sections which were verbatim (down to typos and extra spaces between select words) with incorporation documents of known CIA proprietaries—the differences only reflecting changes in laws between the two incorporation dates.

Not all fronts will exhibit such irregularities, but if you are lucky, there will be something about them that is not quite right, something that raises your awareness. In my case, this list represents only the tip of the iceberg. There were many other indicators, but those listed are more useful here perhaps than the others.

If you determine that your opponents are intelligence community operatives, you probably know why they have an interest in you. Maybe it's your political affiliations, maybe it's your association with matters of national security. For example, you may work for a high tech company in a decision-making capacity, and that company makes products that could be used to develop weapons of war.

Often, interest in you stems from your association with someone they are already interested in—even if only a brief acquain-

tance or casual phone contact was involved. It is even possible to become a target by dialing a wrong number! As strange as this may seem, consider that such casual and innocent events are often used as a means of passing confidential information. In these situations, you will not likely be subject to more than casual surveillance and general investigation and will be safe from dirty tricks or actual danger. Still, you must remember that they may have no jurisdiction and could also be breaking the law in other ways.

If the CIA is on your case, my advice to you is to ignore the matter, and it will go away—even though it might take months or even years! There are known instances where they continued to wiretap and follow "suspects" for up to five years after it was known that their investigation was unfounded in the first place! You might consider confronting them directly and offering full cooperation to demonstrate that you are clean. The problem is, of course, that since they are illegally investigating you, they won't admit they have an interest. "I don't know what you are talking about..." Still, watching them squirm might be fun.

But should their interest in you be substantiated because of your activities or affiliations, you will need to take steps to protect yourself. The agency generally operates as if it can do anything it wants, and generally speaking, it can. If you represent enough of a perceived threat for them to target you for surveillance, they already consider you a problem that needs to be dealt with. Part of their plan will necessarily call for determining how best to neutralize you as a potential problem, danger, or nuisance. This does not necessarily mean your termination, though that deadly solution has certainly been applied in some instances—and must therefore certainly be considered as a possibility in determining your overall strategic response. Termination is typically reserved for instances which might severely damage the organization—chiefly Langley, but perhaps any involved front. It may also be used in the instance of a severe threat to national security. Thus, you should be relatively safe from that eventuality. Still, a good insurance policy is needed, as covered elsewhere...

Other Spies

Domestic spying on American citizens is by no means limited to our own intelligence apparat. Indeed, we are subject to a wide array of players, mostly those working on behalf of our govern-

ment, but there are certainly some who operate in their own best interests. An example of this is B'nai B'rith, the spy arm of the Anti-Defamation League. Simply mentioning them in this way subjects me to being labeled as anti-Semitic, but there are many references in the literature on the intelligence community to illustrate that the fact remains they spy on citizens for political reasons.

Perhaps some of their spying is on supposed or alleged enemies of the Jewish community. However, it has been documented that they also spy for other reasons. It is thought that they are an extension of the MOSSAD, the Israeli equivalent of the CIA. Both agencies, and the spy agencies of other foreign powers, are all capable of spying on you and me without intervention by FBI or law enforcement (and, perhaps, with their blessing). Why?

Usually, it's because our own government agencies want to know what you are doing, but cannot safely do so because of legal limitations. The CIA, for instance, would not wish to be caught violating their charter by spying on American citizens. So what do they do? They ask a buddy to do it. The spy involved, of course, is seldom tracked down to the parent organization itself. If caught, the case can be made that it is merely a civilian spying on another civilian. The buddy agent is willing to do these favors in exchange for other favors. Sometimes files on citizens are exchanged between agencies the way kids exchange sports trading cards. However, it is strictly illegal. In 1992, an excellent example was uncovered by the *San Francisco Chronicle*. They documented in a series of articles that the CIA and B'nai B'rith, as well as Portland Police, were illegally exchanging hundreds of files on U.S. citizens, files mostly obtained in illegal political spying operations.

As reported by the *San Francisco Chronicle*, the *Spotlight*, and former CIA agent Ralph McGehee in his *CIAbase* archives (a rather diverse cross-section of media), Tom Gerard, a San Francisco police intelligence officer (and former CIA agent in El Salvador—which translates into current CIA operative within the SFPD), was indicted for passing confidential police intelligence files to the local ADL office. He worked closely with Roy Bullock, a secret ADL employee of 40 years who was also a paid FBI informant. Because Gerard was illegally meeting with South African intelligence operatives, the FBI investigated served the ADL and Bullock with search warrants.

Bullock's computer was seized from his home, revealing he had

tapped into the phone message systems of political groups to compile data on 9,876 individuals in 1,359 political groups. These were distributed fairly between the left and the right—not exactly subversives in hiding. ADL spying was (at the time) centrally coordinated from New York by ADL spymaster Irwin Suall. Further, a police locker belonging to Gerard contained thousands of police reports on citizens illegally obtained by law enforcement, including files from the Portland Police Criminal Intelligence Division. It soon became apparant that these sets of records were being exchanged between agencies like so many baseball cards.

The fallout was interesting, and the file content, too. Within hours of the article hitting the stands, Portland's Police Chief suddenly resigned without explanation. The local library suddenly decided that the *Chronicle* was no longer popular and removed all copies from its files. The *Chronicle* suddenly found itself being threatened by the Anti-Defamation League as being racist in policy, and there were threats of lawsuits. The articles stopped. The official investigations into the matter at state, federal, and local levels were suddenly dropped, never to be seen again. *The Oregonian*, in Portland, never dared ask questions about either the *Chronicle's* findings or the Chief's resignation, and it certainly never dared to link the two obviously related events.

Nor is the ADL alone in cooperative spying on U.S. citizens as an illegal surrogate for Big Brother. According to McGehee, John Singlaub, a spooky individual with a dark past, runs two such operations, Western Goals, and Political Research Associates (PRA). Operating out of Cambridge, Massachusetts, both are smaller than the ADL. To cite McGehee, "All three groups identify with certain constituencies as a flag of convenience: the ADL with the Jewish community, Western Goals with the right, and PRA with the left." Thus, we see that politics actually have little to do with the spying. The Singlaub case alone reveals that illegal information on citizens is a commodity, one freely traded to anyone with an interest in anyone else's business.

Of more interest in the Gerard matter, with respect to the files from the Portland Police, is the content of the files themselves, which I have seen. Citizens who subscribed to or advertised in certain newspapers with a known political bent were spied upon, for no other apparent reason. Police files were opened by the Portland Police Department's Criminal Intelligence Division on people who seemed to have nothing to do with any ongoing investigation.

One file refers to a skinhead with long hair, which is a strange thought. Come to find out, the skinhead with long hair was a reference to an undercover operative believed to be affiliated with the CIA, who was apparently known to the officer describing him. The officer understood and knew who he was talking about—a man wearing a wig to disguise himself. That man fits the description of one of the people involved heavily in my own spy problems. The nature of the report could be matched perfectly to one specific situation that involved me—but I can't prove it, so I can't do anything about it.

Know Your Allies

Generally speaking, you do not want to draw your friends and family directly into your situation. Of course, some exception must be made. You may want to inform your immediate family or those you live with and those who may already have suspicions or be somewhat aware of your plight. Even then, only call on them for help if they truly understand the reality of the situation and sympathize with you—any doubts they have can harm you greatly if they finally choose to change sides or withdraw help at a critical moment. If your problem is of a legal nature, these people may become involved anyway. Therefore it is better, in some cases, that they hear of your problem from you first.

Women with close relationships to family and friends are often in a better position to ask for help than men in the same situation. It is unfortunate, but a man telling parents or friends of his problems often is discounted to a degree, perhaps under the assumption that he should be able to handle the problem on his own, or perhaps because it is presumed that he is exaggerating. A woman is more often given the benefit of the doubt by those close to her, and people tend to be more protective of a woman in trouble. For this reason, where a couple is in trouble, it may be best for the woman to approach would-be Samaritans. It may even work better if she explains that it is her idea and that he would not approve if he knew. Of course, your knowledge of your own relationships with family and friends will help you do the right thing.

Strangers

You can often approach complete strangers and cry on their shoulder for support in relatively unassuming ways. (Women, of course, can face limitations on who among the males around them they might approach, and how.) I once picked up a hitchhiker and gave him a quick thumbnail explanation of my problem. I asked that, if he felt he was being followed after I dropped him off, he should please call me. He did. Moreover, because he was somewhat angered and intrigued, he wanted to help further. I told him it wasn't necessary, but later, I did call on him for other support at a time when I wished to retain my anonymity. You need not give a stranger complete or even truthful explanation, especially when the truth may sound too implausible. However, you may need to

settle on some form of compensation. Another way strangers can help, if they do know the truth, is to provide a kind of insurance by virtue of "public" or "common" knowledge of your problems. Bad things seldom happen to those who have raised the awareness of those around them.

The Underground

"The enemy of my enemy is my friend." If your opponents are bad cops, corporate bullies, or federal agents, this axiom may prove useful. Almost anywhere you look, you'll find radicals, activists, and organizations who, because of opposing agendas or beliefs, are also set against your opponents. These folks may also have been targeted by your enemy in some way or may already doing battle with them in some form. Perhaps they are experiencing the same kinds of problems as you are or have been "at war" long enough to have developed resources, tools, and techniques that you might find useful.

Keep an eye on the public access channels of your local cable TV, and listen to your local public radio. In larger communities, there are typically a number of underground or anti-establishment groups or people with radio or cable shows (usually live, call-in talk shows). In my area, there are shows which regularly document abuse of power by police, government, and big business.

In an attempt to establish a network of such resources, I encourage you to send me any contact information, or at least, give them my contact information. The wider the network, the more effective it becomes. Cable TV programs are, for instance, often made available to other markets. A program can be routed from one city for airing in another, or if appropriate, copies can be made. You never know what information will be useful or where in the world the source will be.

The same can be said of Internet. My favorite search destination is Dogpile, at www.dogpile.com. This search engine is very flexible and automates simultaneous searches using a long list of other search engines. It can even search Usenet newsgroups for e-mail postings which cover the topic. This can be as valuable as a Web site because you might find someone else out there who has exactly the kind of situation you do or who has exactly the information you need.

A word of warning, however, is due if your entanglements are with federal agencies. Under the new anti-terrorism laws, if you

are out of favor with the FBI, CIA, or military intelligence, you might need to consider this. These new, oppressive laws do away with the whole notion of presumption of innocence and replace it with he notion of guilt by association. If a particular person or group has been targeted under these laws and declared as either a suspected terrorist group or a "potential threat to national security", the government is free to take extraordinary actions.

As a result of the Foreign Intelligence Surveillance Act of 1978 (FISA) and expanded powers granted to the Justice Department and the intelligence community in recent years by presidential executive orders (specifically, Bill Clinton's EO number 12949), most recently in knee-jerk response to the Oklahoma and World Trade Center bombings, you have lost your right to privacy, your protection from unreasonable search and seizure, and your right to a fair hearing. Seven men can meet in a secret court, with no public record kept, to decide that, because of whom you may have associated with (even if accidentally or coincidentally), the FBI may search your property secretly without your knowledge (perhaps, given the FBI's demonstrated penchant for fabricating evidence, to plant evidence for later discovery), take anything they want without notifying you or obligating themselves to return it, and conduct full surveillance on you (perhaps even involving hidden video surveillance in your bedroom). They may even take further action against you without revealing why, what they have done or learned (or believe), or taken without your permission.

They can do this even if you simply associate with someone already targeted. Even if you were to accidentally call such a person and the call was traced back to you, you can be targeted. Individuals have been hauled into law enforcement facilities for questioning and forced to testify before grand juries based no more than this. And if you were to find an FBI agent in your home and shoot him thinking he was a burglar, you will be arrested and charged with murder of a federal agent.

In fact, when government talks about conspiracy involving a particular number of people, they are merely stating that some central core has contacted a number of individuals, who, in turn, have contacted some additional number of people, and so on. They then use these statistics to impress the public and Congress that even more repressive laws are needed to help them fight a "growing problem," and we sheepishly go along with them.

The Professionals

There are several professionals you may wish to seek out. Find those you can trust, for you will want to be able to tell them everything. Lawyers, private detectives, and reporters all have both a legal and ethical obligation to remain quiet about whatever you reveal. Beyond the legal advice they can give you, lawyers can be useful in other ways, often providing references or securing other help on your behalf. And don't forget technical experts, who are indispensable when dealing with electronic bug detection. Just approach any professional with caution, taking care that you do not reveal sensitive information unless absolutely necessary and only if you have high confidence in them.

Groups

The ordained leaders of most churches follow the same code of confidentiality as do lawyers and journalists. The church itself may provide a wealth of people concerned enough to give aid, provided you do not ask too much of them or frighten them needlessly. In addition, many churches have widespread ties to other churches and related groups. One friend of mine in the church was able to gain entry into FBI and Secret Service databases, which allowed me to compile information on active cases that might have had bearing on my situation. Short of having a friend high in the ranks of the FBI, this kind of access would otherwise have been impossible.

Another church-related resource is your personal faith. Without wanting to sound like a preacher, I must testify that my God has helped me through my own times of peril in ways that unmistakably reveal His work. My wife and I asked our pastor to hear our problem and pray for God's guidance and protection—with dramatic results. I know that those who put their trust in God fare much better than those who choose not to pray for divine assistance. There were many times when, without any reason or clue, I found myself alerted to an enemy's presence or action by mere bolt of inspiration—virtually a voice within me telling me that evil was near. This time, I am not talking about instinct. I've been at my desk in an upstairs office and felt the call, walked downstairs into a crowded retail environment in time to find a spook entering the building. I've walked down a frequently traveled hallway and felt moved to go to a restroom door and open it an inch and listen,

only to find spooks conspiring against me. At least once, this kind of intervention saved my life. It is something to think about.

There are many professional organizations and informal groups that can also help. The American Civil Liberties Union, for instance, is a watchdog group for personal rights. In approaching such groups, be forewarned that each has a specific mode of operation and their own agenda, and you might not fit in as expected. A good way to check on a particular organization is to get on their mailing list so you can see what kind of paraphernalia they are distributing. Use your imagination and check the Yellow Pages and the Internet, as well.

Media

Reporters or editors can become valuable allies, especially if you can turn them onto a meaningful story. If you can interest a reporter in your situation, you tap into a wealth of investigative experience and influential contacts and resources. Better still, you may end up with media exposure of your problem, which can help in several ways. By illuminating yourself, many kinds of enemies will run for the underside of the nearest rock to avoid detection and leave you well enough alone. And by calling attention to your problems, others sympathetic to your cause may come to your aid, either because they are in a similar situation or because it serves their agenda to do so.

If your situation is very serious, however, and your opponents are very nasty or powerful, there is a danger that they will become aware of your intentions before you can capitalize on any such exposure. They might see this as an unforgivable escalation on your part which, in turn, might move them to consider a preemptive strike against you to silence any would-be investigation and exposure.

Badges? We Don't Need No Stinkin' Badges!

If you must seek the aid of the law but are uncertain you can trust them fully, take a few basic precautions. Try to seek out a single cop you know you can trust and solicit the suggestions of friends. You might, as mentioned elsewhere in this work, consider getting the name of an Internal Affairs officer and drop that name casually during your initial encounter with an officer you're unfamiliar

with—it can provide just a little extra incentive for the cop to remain on the up and up with you. Document, and have witnesses for, every interaction with law enforcement, and follow up by asking to review any they have that may pertain to you. It is your right to view them and to correct any errors they may contain, unless you are object of an investigation, in which case you may need to use the Freedom of Information Act or some other legal means to access the records. This, unfortunately, will require precious time and money.

General Strategies

You need a game plan. It's likely that you'll only be able to devote part-time efforts to your own investigations and strategies. Your opponent may well be able to throw round-the-clock, multiple-person resources into his, and you can bet he's got a plan of attack. You need take these ideas into consideration and be clever, dedicated, thorough, and cautious. Take some time to think about it, and do it right. Despite your current situation, you will likely have plenty of time for this key step. Don't ever let yourself be rushed unless you have some indication of an impending event which must be addressed immediately.

Knowing your enemy and their motivation is everything. Figure out their M.O. This is half the battle. Use that knowledge against them. Remember, most of these kinds of people are used to dealing with people of average intellect, moderate to low awareness levels, and unsophisticated resources. This often lulls them into complacency and a false sense of confidence which you can exploit. The issues covered in this section will help you in establishing a game plan. Despite the differences in resources and training, you can prevail.

No Monkey Business

Unless you are lucky, you probably don't know your opponents or their purpose in attacking you, and you probably don't yet have a solution to combat them in hand. Just remember, you've got to play the game in order to win the game. This means doing things which are calculated to cause your opponent to make mistakes or take actions that provide the telltale signs of identity and purpose. It's a slow process that could take months, but you'll have all the time you need in most cases, so don't feel rushed or panicked. Look for escalation of enemy resources. Look at the responses to your actions, the defense to your offense. Watch how situations play themselves out. Note any incongruities in what you see or differences from your initial supposition. This leads to an understanding of he enemy's purpose, which, in turn, leads to development of good defensive measures. And if you have your camera or videotape recorder handy at all times, you might just gain some damning evidence to use against your opponent.

The important thing is that this is the time to have fun (inasmuch as you are able to) with your situation. Burning a covert operative when he thinks he is doing a good job not only gives you a good feeling and confidence in your abilities, but it also jabs the other side in many ways. It destabilizes them and puts them off balance. It forces them to become reactionary instead of being in control. It demoralizes those involved on the front line, as well as their supervisors who must report higher up. It forces them to up the ante and makes them reckless.

Once you engage your opponent, don't stop. You need an ongoing campaign to reveal their operations and generate continued escalation while you build an insurance policy. In my case, I elected to enact a direct frontal attack. I wrote a blackmail letter! I wrote it anonymously and took care to make it as generic as possible, then arranged for it to be mailed from another part of the country, using the return address for a former CIA proprietary. The letter accomplished several useful things.

First, any response directed toward me would prove that I had been their target—for only my opponents would know to fit me and my circumstances to the letter—which otherwise had no clues whatsoever as to who sent it. In fact, only my opponents would even know my situation. Second, though it was deliberately vague, it hinted at information I had that could harm them. The test was devised so that they would respond only if my information was accurate. They did respond, and it was proof that I had indeed found my antagonists while simultaneously achieving a useful insurance policy.

Furthermore, their response was to send in their number two man from the organization—someone I had already identified and, better yet, felt I could trust perhaps more than any other. When he arrived, he teamed up with a known operative from within local law enforcement. By capturing the two of them together on video, my "insurance" became very solid, indeed.

Business as Usual

If you can get this far, with your opponents identified, their aim determined, and your insurance established, you can probably begin to go about your business again and get on with your life. There should be no further reason for difficulties between you, especially if you actually sit down and negotiate resolution. In my

case, and perhaps in yours, this may not even be necessary, especially if you hold all the cards.

This does not necessarily mean that they will not continue to watch you, nor may you stop watching them. But as long as you do not appear to be going to the authorities (very foolish), you will remain safe from serious trouble. This is the time at which you should stop letting them know you have blown their operations. Just quietly take note, and go on about your business. Smile inside.

Dangerous Liaisons

If you must meet with your opponents in other than an "official" way, say, with your lawyers present, you're probably at risk for some nastiness on their part. Generally, if it is on your terms and your opponent has some degree of respectability to protect, if and others know of the meeting and are ready to blow the whistle if you do not return, then it is safe to meet. Certainly, the quality of your insurance policy plays a key role. I have frequently felt comfortable walking unannounced right in the front door of the offices of CIA proprietaries. Not only was it interesting and informative, but actually, it was extremely fun to watch them fall out of their chairs...

If you sense a potential for risk, there are things you can do. Choose a place which is more or less public but where the meeting would not draw attention or be easily overheard. Advise that you will have your back covered in several ways but that you will not be involving the authorities. And unless you are certain your opponent is unsophisticated, do not attempt to violate your agreed conditions in any significant way. If they tell you that you had better not be wired, you can bet they'll check. If they say "no cops", it's best to comply.

Generally, it is better to choose the site (well in advance of needing it), and be the first person there. If you are to meet at a sit-down affair, such as a restaurant, choose a corner table where you can see all entrances, and have a place nearby where you can duck to safety.

Give them a false time. "I can't leave here until I get a baby-sitter—so make it in three hours..." Then, get there pronto, and watch from a distance for signs of their own early arrival. They will likely check the site out, which should be expected, but if you see any signs of preparing a trap or other violation of terms, you

should be a no-show, and don't be polite in explaining why. They've just given you the upper hand; if they want to try again, you can afford to be indignant and demand concessions.

On The Run

If you are on the run, or if you are about to run, the key thing to keep in mind, always, is that you must at all times be ready to run again. It is best to establish two safe houses: one near and one far. Also establish a decoy safe house location and corroborating evidence.

A safe house will typically be a home or business where you can flop temporarily. Find someone from your past or very peripheral to your life; someone who would help if your were to call and simply say "If I turn up suddenly one day, can I stay the night or a few days while I get my act together?" Use your time at the safe house to plan for your future, whether it means resolving your current dilemma or preparing a new identity and a new life—and don't stay long! You owe it to your host to leave as quickly as possible.

In preparing your decoy safe house, pick a city or country and not a specific address. Make observable but "covert" inquiries to travel agents and have them mail you brochures for three possible destinations. You need to make your enemy work to figure out where you will run to—or where they will think you will run to. Hide the brochures after making notes about monetary conversion rates, hotels (suggest at least a half dozen) and room rates, and perhaps a common personal last name along with the name of a large corporation with offices there. Place some long distance calls to that company's personnel department from a pay phone you believe they are monitoring and ask for personnel, that they might send you some employment applications, or if you are currently safe, from your home (they could check your phone bills.) See Appendix III, "More About Bugs," on electronic surveillance for more information about wire taps and other eavesdropping devices.

Lastly, do not make contact with anyone at home unless you have established a foolproof code system. Whatever communication you make must be coded so that discovery by the enemy will not result in suspicion—make it look look and sound like a marketing offer or something along those lines. Find a way to obtain some corporate envelopes, literature, and stationery from a local

firm not related to your life and mail your coded letters that way. Better still, use a computer bulletin board service (BBS) or Internet newsgroup to post coded messages. Be certain that your contacts send and receive messages other than just ones to and from you—and whatever you do, make contact only when it is important. Better still—DON'T DO IT AT ALL!

Awareness is the First Line of Defense

With proper attention to what is going on around you, you'll be forewarned of any possible danger or unwanted activities on the part of your antagonists. This knowledge will allow you to take actions which enhance your position, and weaken your opponents position. At the very least, it can buy you time and give you more options and opportunities. Don't worry if you don't win early on or if you lose a few skirmishes. A series of small victories over time can ultimately lead to total victory—especially if your opponent is operating illegally in any way.

Therefore, be alert. Take note from time to time about what's going on around you. Repeat occurrences or odd behaviors are indicators that something may be afoot. People don't usually sit in cars for hours on end at the curb. Strangers don't usually end up in your rear-view mirror both on the way to and the way back from a destination. It isn't normal to get a lot of calls where all you get is silence on the other end of the line and then a dial tone. It isn't likely that important mail would be postmarked well before actual delivery, while junk mail is delivered on time. Objects in your desk at home or work should not be rearranging themselves in your absence. These are warning signs.

Make a habit of remembering or keeping track of the small details in your life. Take steps to deliberately create details which are easily remembered or tested for. I call these "trip traps." Is the pen in the glove compartment still under the first piece of paper and the owner's manual upside down? Is the stack of paperwork on your desk still arranged so that the corner of the upper page touches the tail of the letter "Y" on the first line of the page underneath it? Is the toothpaste tube still facing the same way with the same dents in it?

You can also set traps. Trap small items in between moving parts which will dislodge when operated. Wet tissue or strands of hair can be used as "seals" on entrances or storage openings. Use spring-loaded mechanisms which dislodge in a way that cannot be reconstructed easily. There are endless variations to these kinds of indicators. The best indicator is one which is undetectable, but often, you might wish the opposite effect as a "gotcha."

Survey the situation, and ask yourself a few questions. Might

your opponents delay you with vehicular sabotage? If so, check for foreign objects wedged in under your tires. Do you have a locking gas cap? Place a piece of clear scotch tape into the crack of your trunk or hood (or gas cap). Keeping a hidden spare set of ignition cables and distributor cap and a diagram of their installation might be wise. Might your antagonists be inquiring with work associates, friends, or family about you? "Anyone been asking for my phone number lately?" "Has anyone been asking about my trip to Seattle?" Might your adversary be out to harm you financially? Check your personal credit report on a regular basis, and challenge any errors.

Predictability vs. Unpredictability

Part of your game plan should be to address the issue of your personal habits and patterns. Your opponents will be quick to recognize any such regularity. But you can do the same with them. Establish what level of predictability you can expect of your opponents. Make a check list of what you can reasonably expect them to do. Don't hesitate to include things which may seem far-fetched (such as law enforcement's use of illegal wiretaps). There are many things you need not worry too much about. It really makes little difference, for instance, if you are being followed regularly, except when you are trying to meet someone covertly.

Second, you must become attuned to your own predictability. Make a checklist of what you do on a regular basis that your opponents might be aware of. Do you go to bed and rise at the same times? Do you take the same route to work each day? Don't make the mistake of letting your antagonists know more about your habits than you do.

Rate each habit in terms of sensitivity or risk exposure. Unless the risk associated with your circumstance and the particular activity is high, you will not likely want to change your habits. Change, in itself, is not the answer. Knowing when and why to change is. Note ways you can change, taking into consideration if such a change will require advance planning. Will you need to apprise others, for instance? How can that be done without your opponents being aware? Is it possible for the change you plan to reveal your intentions, and is that good or bad?

With this information in hand, you can use your own predictability to your opponents disadvantage. When they expect

you to zig, you can zag—only if it is worthwhile. Consider these generic possibilities: Altering your habits to suggest that you are doing (or planning to do) something or that you have stopped doing something. Alter your habits in a way that suggests you know they are doing a particular thing—forcing them to change methods. This can be a key tool in determining your opponent's identity and limitations. Likewise, your opponents may know your limitations and anticipate your possible actions. If you don't have a car, then your mobility is limited and therefore more predictable. If you don't have a home alarm system, your defenses are *perceived* as being weaker (remember the trip trap?).

Contingency Planning

Try to project what might lie ahead for you, and have a contingency plan in mind. Whether you are planning strategy, such as deciding whether to take legal action, or a minor detail like the route you take to work, try to formulate exactly how your opponents might act at any given time, and have in mind a way of making that work to your advantage—or at least minimize their gain. Know what you are willing to do. For instance, you might rule out a contingency that would mean committing a crime. Consider that anything you might do may be anticipated, and plan actions which seem unlikely for you.

Resources and Props

Early on and then from time to time as your situation changes, you should make a checklist of your resources and props. A resource might be money or an ability you or a friend can apply, such as desktop-publishing skills or access to a printing press. A prop is usually physical hardware such as a multiband radio scanner or dependable transportation that the enemy does not know about. Consider just how each resource can benefit you. You may even wish to consider the order in which you use your resources. Don't rule anything out just because is sounds outlandish or weird. It won't hurt you to consider it, and you can then decide later whether to use or discard it.

Photography Gear

There will undoubtedly be times when you will benefit greatly by countersurveillance, which can make you aware of your opponent's presence and by which you can document the "oddities" you may discover. These may allow you to determine the relevance of suspicious goings-on. Such evidences could prove useful in providing you with insurance against harm, or it could potentially be used in court actions you may wish to take against your antagonists. It can become part of an overall insurance policy.

I'll resist the temptation to launch into a diatribe of why you should spend $10,000 on the finest array of cameras and peripheral equipment. All you really need in most cases is a good, inexpensive camera with a telephoto lens—something small and easy to carry, with autofocus if possible. You will generally want to point and shoot in a way that will not require bringing a camera up to your eye and focusing. Generally, unless you are trying to frighten off or burn an operative, you don't want to call attention to the camera. In fact, it's better to miss an opportunity or fumble a shot than to reveal the tactic. Inexpensive fixed-focus telephoto cameras are available in both disposable and 35 mm pocket versions. Choose a camera with a self-timer.

A 35 mm camera is the better choice because it lets you choose faster film for low light work and accepts longer lenses. If you have a 35 mm SLR with interchangeable lenses, I recommend a 200 mm lens for the bulk of your work, the perfect choice being the compact 250 mm mirror lens. Generally, you will not need wide-angle or normal lenses. The possible exception is if you need to photograph an interior room, where a wide angle lets you do it with fewer images. An interesting and excellent choice, if you're willing to spend a few hundred dollars and the time to find one, is the discontinued Olympus Pen 35 half-frame camera. It gets twice as many shots on a roll, and was the smallest interchangeable-lens camera available commercially. For that, a 135 mm or 150 mm lens is as long as you might need, and it can virtually be palmed out of sight until needed, or even hidden in a coat sleeve taped to your wrist—operated while "looking at your watch".

If you intend on doing your own darkroom work to avoid unwanted eyes seeing your pictures, I suggest two B&W film/processing combinations. Kodak high-contrast copy film, when processed in Kodak HC-110 developer, can be pushed to ASA ratings of 2,000 and beyond for ultra-low light photography. The same

developer can also process Kodak infrared film, which can take usable pictures in virtually pitch-black conditions—especially if you have an infrared flash or other infrared light source (such as "active" night vision equipment). The results will be grainy but have sufficient detail for your typical needs. These items can only be purchased from professional or industrial camera outlets. The film itself is usually purchased in 100 foot rolls, requiring you to load your own 35 mm cassettes with a bulk film loader—giving you the advantage of putting anywhere from 6-40 shots on a roll depending on your needs. Shorter rolls let you switch between film types without waste, and longer rolls offer convenience on extended shooting sessions. This is all fun stuff, by the way, and I encourage you to get involved with photography for that reason alone.

The other way to deal with countersurveillance is with video. A number of super-8 video cameras offer excellent size and features for the price. Or, if you have a serious project need, a few systems offer interchangeable lens capability, often accepting 35 mm camera lenses (which dramatically increase the effective focal length by a factor of 4—a 200 mm lens performs like 800 mm).

Keeping a small camera or video camera handy at all times is a useful tool. Generally, you don't want to be seen taking pictures. With practice, you can learn to take pictures without raising the camera to your eye. Focus and exposure can be preset (or be fully automatic on some models) and just aimed in the direction of your subject by casual body movements.

On video cameras, I like to paint over the LEDs. Ideally, I would also install a switch which cuts power to the viewfinder display when desired. This not only makes the camera more undetectable but also extends battery life significantly. Another feature I like is a good stop-motion or still-frame capability. Some cameras have a time limit in this mode, so choose wisely.

Photos and videotape can often be an important prop. You can sometimes use these as bait, labeling them for best effect. I often like to be seen with my camera, then later refer to incriminating images (sometimes even when they might not exist), and then wait to see what happens next—ready to document it. Evidence, like truth, is often not black and white but, rather, based on perception. There are times when the perception of "evidence" is more important than the reality of it.

Tape Recorders

This is another important tool for documenting events. I like the very small microcassette systems with automatic voice activation. I put them in my shirt pockets so that I can record descriptions of vehicles, people, or events without pen and paper. This means no hands required (extremely helpful when driving), and no paper trail. I can leave notes to myself on ideas or research to follow up on at a later time. And if anyone should engage me in conversation—I have it on record without having to do anything special. I can later transcribe these into a computer database and easily search for matching occurrences. In this way, I don't have to have total recall, and I can broaden my base of vehicles or people considered as possible bad guys.

Consider getting a number of these little gadgets. You might keep one by the phone with a microphone already attached, needing only to be turned on to record conversations. (Check with a lawyer about the legality of recording conversations—in most areas, you should find that it will be legal if at least one person involved in the conversation knows about it or the recorder was already running when the event began.) It is sometimes beneficial to leave them on in key places to see what takes place when you are gone—a trick equally useful with video cameras. Leave them at home and at work, even in your vehicle. If you cannot hide them well, consider disguises. I have modified several items such that they appear to be ordinary objects of other purpose: a cheap camera, hand-held scanner, radio, etc.

I simply take the original object apart, remove the guts or replace them with a miniaturized version (so the radio still plays, for instance), and put the recorder or camera inside—perhaps with its external case removed to further conserve space. I use Scotch double-sided tape to hold it secure or pad the excess space with foam rubber. Sometimes you can modify the outer product's buttons or controls to manipulate the controls of the hidden unit, but this is not normally important when you've got voice activation or a timer. I then run an external mic either to a logical opening in the outer product case, or I'll disguise it externally.

I like to use lavaliere mics, the kind that are normally clipped to neckties. These can be built into almost anything. One set I constructed, for instance, is a Walkman-type radio with headphones, which I can wear constantly when needed, sometimes adjustments to the volume or bobbing my head to the music. When I need to

talk with someone, I remove the headphones and let them dangle about my neck—the perfect location for the microphone built into one of the earpieces.

The other way of using such fake machines is in playback mode. I have prepared in advance a sequence of "communications" messages on tape. Using the a walkie-talkie with a hidden internal recorder, I was able to fake talking with companions. Following a memorized script, I would talk into the unit and then play the "response." Tailor the script to best manipulate your opponent. With the aid of other props such as false ID or clothing, you can also use this technique to reinforce a false identity.

Fake ID

It is illegal to have false identification. However, it is not illegal to have an assumed name, and to have identification under that name—such as an author writing under a pen name. You can carry informal ID such as business cards or credit cards under any name without violation of the law. Just don't have a lot of credit cards under a lot of names—just one, perhaps, with a reasonable story as to why you have it (found it, borrowed it, whatever). If you are going to have a false ID, it should be kept in a separate wallet to avoid the possibility of two sets being displayed. Again, if the second wallet is discovered, have a reason for its existence. Arrange with a friend to verify your story. Let's face it though, even if you're carrying a false ID, you'll most likely never get caught, let alone get in trouble for having it.

Fake business cards can be used to garner information. Secure or manufacture a wide variety of business cards in diverse occupations. Presenting a business card as a food inspector in a restaurant will make a waitress or owner much more cooperative in answering questions about a client. And you can get just about any information you want if you pretend you're a doctor inquiring about a patient.

If you must go on the lam, having a fake ID may prove to be an essential part of your escape. Depending on who you are trying to escape from, you may get by without need for false ID, or you may need ID suitable for obtaining employment without using your real name—or anything in between. There are books on fake IDs that can address this better than I. Be careful, though, for with today's holograms and magnetic strips, concocting a fake ID yourself is becoming virtually impossible.

Computers

If you've gotten by this long without one, you may not absolutely need to go out and buy a computer, but at the very least, it does help to have written transcriptions of compiled notes and observations, organized within a searchable database. Like a camera, a computer can be a useful tool for preparing or presenting evidence. Keep in mind that the security of your electronic information is a prime concern, one which is covered elsewhere this work.

One of the prime uses for computers these days is for research via the Web. You can surf the Web to learn a lot about potential antagonists or conspiracies in which you may have become enmeshed peripherally. You can track down contact information on individuals, companies, or resources for information, products, and services. It is an inexpensive resource for aid in self-defense.

Here are some places to start. It's annoying, but the fact is that Web sites come and go, so some of the material here may be obsolete by the time you read this. You should be able to find new sites that have come along to fill the void, however. I'll start with some of the more interesting search engines and sites I've found. I won't bother mentioning all of the better-known search engines, the ones that your Web browser takes you to when you click on FIND or SEARCH.

www.albany.net/allinone An eclectic collection of hundreds of search engines categorized for convenience. From here, you can find almost anything you want, including some of the others listed below.

www.dogpile.com My favorite search engine, one used so frequently that I make it my home page (your Web browser will let you make any Web page your default home page). What I like about it is that you type in your search word or phrase, the engine submits your search criteria to dozens of other popular search engines, and it returns the findings for you in a logical and useful way. It also lets you specify to search the Web, newsgroups, or other categories in whatever combination you specify (more on newsgroups in a moment).

www.nashville.net/~police/risk A Web site which features questionnaires which allow you to evaluate your risk of being assaulted, murdered, or burgled, with advice on how to increase your odds.

www.naa.org/hotlinks/index.asp A resource for reaching many of the nation's leading newspapers online. You can access recent and historical articles as well as contact the editor or place advertising.

www.disinfo.com An award-winning site that specializes in tracking and revealing conspiracies and intelligence-community goings on. They feature a very interesting and powerful conspiracy search engine, which can also be found on my Web site at www.proparanoid.com. Also check out www.konformist.com for interesting conspiracy news.

www.sec.gov The Federal Securities and Exchange Commissions Web site, where you can type in the name of a business or person affiliated with a partiular business and get a ton of financial background data and business affiliations. You can learn about plans they are making and problems they have experienced. This is especially useful if your opponents seem to be under corporate sponsorship.

www.halcyon.com/dagger An excellent resource for books on the intelligence community and self-defense.

www.webcom.com/%7Epinknoiz/covert/ciabase.html The home of CIABASE, an excellent online search engine. There, you can purchase its entire database on floppy disk, complete with the full search engine. This service comes from one of my allies, a former CIA agent turned critic, Ralph McGehee, who served for 25 years in the CIA. Having compiled the ever-growing CIABASE, as well as written the book *Deadly Deceits*, McGegee is a recognized authority on the CIA who has testified many times before Congress and in the courts and who has appeared numerous times on radio and TV.

www.fas.org The Web site of the American Federation of Scientists, the folks who brought us the Nuclear Holocaust Countdown Clock—how many minutes or seconds before doomsday. They also track the errant ways of the intelligence community and other interesting news.

www.netaccess.on.ca/~cirrus An excellent resource for mind control issues, as is www.trufax.org/menu/elect.html.

intelweb.janes.com The home of the famous Jane's military books. Jane's now also tracks the intelligence communities of the world. Of course, Jane's is in business to sell its books and services, so they don't give away too much information on the Web. Still, it's a great site.

www.loyola.edu/dept/politics/intel.html An interesting collection of links related to the intelligence community; it includes information on the intelligence community's official Web sites.

www.logos.it/query/query.html An unusual Web site that can be used to translate a given English or foreign word back and forth into any of 30 languages. It's not only useful, it's fun and educational.

www.cs.virginia.edu/~alb/misc/moreMindLinks.html A collection of information and links on the intelligence community with emphasis on mind control and excellent material on CIA control of media.

www.tscm.com/giindex.html and **www.amug.org/~dbugman** The Web sites for James Atkinson/Granite Island and Tim Johnson/debugman, technical-security countermeasures specialists. These are among the best techs available in the field of detecting and defeating electronic surveillance—and they have put together excellent informational sites that you will undoubtedly enjoy.

Also survey Appendix VI for useful websites. In addition to Web sites like those above, newsgroups offer a great resource and a means of contacting other people with similar interests or problems. You can find newsgroups on thousands of select topics, where anyone and everyone with an interest can put their two cents in—for whatever it may really be worth. Your Web browser has a menu or button which will take you directly to the newsgroups—but you may have to scroll down a long list until you find the name of a newsgroup you're interested in. Like Web sites, they are subject to evolution and change, so if the newsgroup does not appear as current, you may still have to go hunting.

alt.conspiracy Offers a set of over twenty newsgroups devoted to conspiracies. Some of them are far-fetched, while others are contemporary and historically accurate—everything from alt.conspiracy.abe.lincoln to alt.conspiracy.yakworshipers. The problem is that real spooks often hang out there to try to keep people from disclosing things they don't want you to hear about—usually with good reason. They also hang out in the next set of newsgroups, alt.politics.org, which offers a series of insider/outsider interactions with respect to specific federal agencies, such as the FBI, CIA, NSA, and BATF.

alt.politics.org.cia My personal favorite. When I'm not too busy with books or other projects, I try to hang out there and keep folks (and spooks, especially) honest.

www.dejanews.com A search engine dedicated to finding anything said on any of the newsgroups. It is a very impressive tool that can help you find who has said what, when, and so on. Terrabytes of information which, I must point out, will also keep track of anything YOU say on the newsgroups. So remember that anything you say can come back to haunt you. Don't speak unless you're that certain that what you're saying is something you want to be recorded for posterity.

Paper Shredders

You probably should have a paper shredder, even if just to make the other side think they missed out on something and that you regularly have papers they might like to know about. But unless it is a very good one which crosscuts and you have tons of similar-looking material, I suggest you also burn the shreds—it makes fine kindling. A good and determined opponent with unlimited resources will happily throw those resources into reassembling of a shredded document. Don't think it can't be done.

Dummy Drop Box or Mail Box

It is often desirable to have an address at which you can retrieve items which cannot be safely mailed to you directly. This might be a commercial postal box or even a regular post office box, or it might simply be the address of a friend. Sometimes, however, you

need an address that cannot be traced to you at all. There is a way, though you will not likely be able to maintain it for long periods. Look for a trailer court or apartment complex which has had a vacancy for some time. Trailer courts work well because they often have mailboxes set up for all possible trailer combinations based on single-wide trailers. Voila. Just drive by regularly and pick it up or have someone you can trust do it for you.

Portable Communications

Your opponent may well make use of portable communications, and so might you. With a cell phone, you're only seconds away from placing a 911 call. One or more sets of inexpensive walkie talkies can be shared with neighbors, family members, or others willing to help. A pager system can be used as an early-warning system when involved parties use predefined codes as return number entries. Again, cell phones have their own associated security problems, also described elsewhere in this work. Walkie talkies transmit on radio frequencies, which anyone can listen in on, so you may want to devise a code beforehand. Such a code can be spoken words or even just clicks of the call or mic button, which produce audible sounds at the other end. You might use two clicks to warn that someone is coming, or three to suggest that the emergency plan should be enacted.

Be Prepared

There is a long list of things you might wish to consider for any contingency: medical kits, roadside-emergency provisions such as a tire iron and jack, fuel reserves, firewood, food and water, emergency power generators and batteries (and battery-operated radios, televisions, communication devices, alarms, etc.), tool kits, spare auto parts (distributor caps, spark plugs, fan belts, locking gas caps), flashlights, and camping gear. More atypical but essential for sudden escape are stashes of cash, false IDs, passports, maps of key places, weapons and ammunition, etc. You might want to invest in rare coins and jewelry, items which can easily be liquidated for large sums but can be easily hidden and transported. Other sections of this work give more in-depth coverage of other aspects of preparedness, discussing items such as night-vision equipment and security systems.

Mace: the Good, the Bad, and the Ugly

Mace is a form of tear gas. Pepper spray is a less potent alternative to Mace. The nature and purpose of such products is to disable an attacker and, in most cases, incapacitate them while you obtain help. It doesn't guarantee success, but under ideal circumstances, it will render the attacker temporarily blind and incapable of using his full lung capacity. It can cause severe discomfort and burning that can bring a grown man to his knees. This can, however, take several seconds, and the Mace user must be prepared to retreat or defend his/her position momentarily. Be cautious, for if you are already under attack, you may not be able to produce, prepare, aim and discharge the product effectively, and, worse, your opponent could gain possession of it.

Use of defensive sprays (or any weapon, for that matter) should not be undertaken lightly. Spraying someone with Mace is illegal except in self-defense. If you are not fully justified in your reasoning, you can be arrested and charged with assault, and you face the grim potential of a lawsuit from your "victim." Of greater consequence, be aware that the use of any kind of defensive weapon can result in death. Mace, for instance, can cause the victim to suffocate or, under the right physiological circumstances, have a heart attack. You have a right to defend yourself, but any use can have serious repercussions. Check with your local law enforcement

before you go out and buy it. In some states, it is illegal to own Mace, while in others, only milder forms are allowed. In some states, licenses are required, while others may have no restrictions at all.

Over 100 companies make similar products. Mace itself, however, is manufactured by Mace Security International, 160 Benmont Avenue, Bennington, VT 05201; tel. (800) 639-4530. Take care when purchasing Mace or similar products. Buy Mace only through an authorized sellers or competing products only from a reputable dealer. If you purchase a product that exceeds specification, you could be held liable for any resulting health problems, disability, or death if it can be shown that you did not take reasonable care in purchasing.

Retail outlets that sell Mace may include department stores that carry guns, gun shops, sporting goods stores, locksmiths, and hardware stores. You can mail-order Mace from the Police and Correctional Products Division, 439 Main Street, Ste. 3, Bennington, VT 05201-2158; tel. (800) 785-0100.

Bait and Switch

There will be times when you will need to trick your opponents in one way or another. There are three basic ways to achieve this. One is to simply outdistance and outmaneuver a tail. In addition to simply outdriving your unwanted friends, this can accomplished by switching vehicles or transportation.

Another way is to lose your identity. If you are relatively certain that your opponents are only watching your building you are in and have not bugged your home, you can change clothes, don a disguise, and leave. Use a mode of transportation other than the one you arrived by. It is often to your advantage to switch identities with a friend, perhaps having them exit ahead of you or undertake observable activities in a way that distracts your opponents without revealing the switch. This can also work well when used in an airport or bus terminal. You can buy a ticket, board, and then depart disguised as someone else.

Change your age with clothing, a gray wig, a full beard, heavy glasses, a hat which sits low on the forehead. Stoop, move slowly and deliberately. Many people can effectively change their sex with a wig, the right clothes, and some makeup, accompanied by a change in body language. With costume-shop makeup kits, you

can add scars, moles, and other identifying characteristics which superficially distract onlookers quite easily. With some development of skill, you can change a Caucasian skin color to that of an African American or vice versa. Alter your walk and create nervous habits and mannerisms to flesh out your new identity.

The final method is to be in two places at once. Record your sleeping habits or daily routines on audio tape. You might want to edit the tape a bit so your eavesdropper won't recognize a repeated passage. Then, making sure no one can see you, play the tape. You are then free to sneak out and play. Naturally, you can combine any of these basic methods.

The Kindness of Strangers

When in a predicament, strangers can seem like a fallen tree on your road to freedom. But they need not be seen as a stumbling block or even as a completely neutral entity. Let's assume you are being electronically surveilled, and you receive a call from someone who has dialed a wrong number. Just at the conclusion of the call, after having essentially denied all knowledge of the caller or person he or she was intending to call, say goodbye to the party at the other end—by name. Say something like, "Thanks, David," then curse as if having made a mistake, and hang up quickly. Your eavesdroppers will assume that the call was likely some sort of coded message and that acknowledging the person at the other end was a slip up on your part. Playing safe, they will devote precious resources into finding your "David." It works just as well to call someone and pretend you dialed the wrong number. End the call the same way.

Another way to confuse the enemy with the aid of strangers is to prepare a bogus letter from the manager of a good restaurant in town to, say, a radio station sales or promotions manager that simply states that the letter entitles the bearer to dinner for two. Do what you can to make it look official, with return and delivery address, signature, etc. Put it in an envelope and stick it in your pocket. When you know you are being observed, take a circuitous walk downtown, as if trying to be certain you won't be followed. Stand and wait nervously on a corner, looking about frequently. Check your watch and pace.

After a few minutes pacing and looking around you, pick your red herring. Look relieved, take one more quick look around, and

then walk to greet him almost as if you know him. "Hi. Do you live here? Great. Say, I'm from out of town, here on business. I met with a client yesterday who gave me a coupon (at this point, pull out your letter)—good for a free dinner at such and such restaurant. Unfortunately, I can't stay in town, but I'd hate to see it go to waste. Would you like it?"

It doesn't matter if they take it or not. While you're talking and he is reading the letter, look about nervously once or twice. If he has accepted it, leave quickly in the opposite direction from HIS original travel, once more taking a circuitous route back to your point of origin. If he rejects it, act as if he has just warned you that you were being watched. Look about very quickly, stuffing the letter quickly in a pocket with abandon, and immediately act as if you had never even spoke to the person. Change direction, and walk briskly away, once more with the evasive route back to your vehicle. The assumption will be that your contact felt you were under surveillance and that you both aborted your meeting.

PROMIS and Other Lies

There are many ways in which federal agencies can track you online. One of these is software called PPOMIS, used by almost every local, state, and federal law enforcement agency. This was reportedly modified by the CIA to include programming "back doors," which allow illegal access to almost any public governmental system online. It might explain why, on three separate attempts, exactly three days after back-channel communications with the FBI requesting help (the FBI has jurisdiction over any illegal domestic actions by the CIA), that my CIA friends vanished for a couple of weeks, only to return with more sophisticated and difficult-to-observe techniques. PROMIS is even tied into similar systems internationally, having been sold to foreign governments as a panacea for bureaucratic data management. Therefore, if you call a police department or federal agency and they enter your name into a computer, the CIA knows about it. They can even alter the information. Who knows, you might suddenly be listed as "armed and dangerous."

Federal cops and the CIA can also access airline reservation systems and be alerted if someone they're looking for purchases a ticket. Best to purchase it with cash under another name. If your destination is in another country, keep in mind that customs and

border checkpoints also check these systems. Try to travel under a visa obtained from the host country under another name, instead of an American passport in your name.

If you buy a gun from a gun dealer, or if you must see a doctor because of a gunshot wound, the police will know about it within hours. Buy your gun from a private party, and get a signed receipt with proof-of-seller ID. You don't want to buy a gun used in a murder and have no way to prove you didn't have the gun at the time of the murder. And if you do get shot, try to tend the wound yourself or with help from trustworthy friends. If you must see a doctor, have one call on you—don't go to a hospital, and call from anywhere but your home. That will buy you time, perhaps enough to arrange for a good story or to relocate.

If you run vehicle license plates at the DMV, be warned that the plates of federal and local cops and intelligence operatives are likely "blocked." Blocked plates are flagged in the computer to tell anyone who inquires that they belong to someone who is working for the government on sensitive matters and that information on the plates is not to be given out. You will be told that they can't find any such plate registered. Your inquiry on a such a plate is then reported to the agency which requested it blocked. When you run a plate, you risk letting the other side know.

DEFENSE AND OFFENSE

When anyone thinks of cops and robbers, private detectives on a case, or spies, they think of all that action-adventure stuff—guns, bombs, car crashes, fistfights. Forget it. Unless you are in serious, big-time trouble, don't worry about all that.

Once you're accustomed to your opponents' habits and behaviors and have "trained" them on yours, then you will likely know if and when to be alarmed. There comes a point in time in which it's best to relax and flow with the situation. Let them follow you, let them bug you—and use it to your advantage. In doing this, you establish a peace treaty of sorts. In calm times, you can keep tabs on them as much as they do on you—if you do it without drawing attention to that fact.

During this time, compile evidence and document everything, but do not hold onto the material and let them to discover how much you really know. That will earn unwanted escalation, and at some point, you won't be able to keep up. So until you have laid the foundation needed to build a life of freedom, "keep them right where they want you", and flow with the forces at work around you.

Information Gathering

All of the same avenues are open to you as would be to any private investigator. If you have a license plate, you can run it through the DMV and find who it is registered to and where they live. Tax offices maintain records on real property. With an address in hand, you can find out if your suspect owns or rents a particular property. You might be able to obtain a copy of the deed or information on financing. It will tell you the tax bill, and working backwards with tax-rate information, you can estimate the appraised value of the building. If the suspect is a renter, you can find the landlord. Call the landlord and act as if you are inquiring about the suspect, whom has applied to lease an apartment from you. You might not only be able to gain a little information (How long at that address? Monthly rent? Good tenant? Pays on time? Where employed? Wife/children? etc.) but you might also cause him some strife with his landlord.

Talk to people who know your enemy. Be clever and personable. "I think we have a mutual friend, so and so. I understand you know him such and such place. Did you know him when he

was...?" With this information, you can make do all sorts of things, such as make information appear that suggests the suspect is a target of his own people.

If you're looking for information on a business, check with the Better Business Bureau, the City Business License people, the State Corporation Commissioner, County Tax Office, and any professional organizations they claim affiliation with. Check with competitors and neighboring businesses. Somewhere in all of that, you might learn something. Look for information on partnerships, additional mailing addresses, agents of registry, legal counsel, name changes, and so forth.

With names in hand, you can go down to the County Clerk's Office and find out if there are any histories of court or legal proceedings on file under any of the involved names, personal or business. Following up on these may uncover a wealth of information and additional leads: name changes, divorces, lawsuits, criminal records, traffic citations ... everything is right there. Some of these can become goldmines of information. Imagine the likelihood of contacting someone who has sued your enemy and would NOT want to help you.

Somewhere in all of this, you might even gain Social Security information. Knowing that and their address, you can write letters to creditors, credit bureaus, and the IRS. It's illegal, but you could request copies of the last five years' taxes from the IRS (to your dummy P.O. box) or file a change of address with creditors and Post Office so that your enemy's bills stop showing up.

Insurance Policies

If you know what your opponent wants or have incriminating evidence against him, you have leverage. Plate numbers, photographs, witnesses, recordings, etc., all serve to give you leverage. Once you have acquired any seriously damaging piece of information, don't hold on to it. You would hate to see it vanish or, worse, be replaced by altered, unusable material. I recommend that any condemning information you hold be distributed as widely as possible.

A good way to accomplish this is through your church. Find out what other churches your church is affiliated with, and obtain the membership rosters for of all of them. This should give you hundreds of names. Put copies of evidence into a number of envelopes (I arbitrarily choose to do 15 sets of envelopes). With all of your

labels turned face down and mixed up like puzzle pieces, randomly select and attach them to the envelopes. Deposit the envelopes in the mail without being seen, if possible. The extra, unused labels should be burned or put into a sink full of dishwater to soak for a while and then sent down the garbage disposal, where they cannot remain intact or ever be reconstructed. No one except the recipients will ever know who received your materials.

The mailers should consist of a sealed envelope and a cover letter. The sealed envelope should contain instructions to be followed only in the event of circumstances you specify—such as your death or mysterious disappearance, even where foul play might not be suspected. The letter informs recipients of your policy in generic terms, letting them know that you fear for your safety and seek their help. Emphasize that they are in no danger, for you ask nothing of them that they cannot do anonymously. Ask them to help by holding onto the envelope and watching their church bulletin board and the newspaper for any sign that harm has come to you. If anything does happen, they are to open the envelope and follow the instructions.

The instructions should cover several key points, and a list might look something like this:

1. Write a letter to sister churches notifying them of my death, disappearance, etc. and ask for the letter to be posted. (This will ensure that total strangers at other churches will also know when to act.)
2. Please read this contact list (which you have included) of all police agencies and media resources which might logically investigate any possible foul play (FBI, state and local law enforcement, the ACLU, local and national TV news and investigation programs, local and nationally prominent press, local and national political figures, etc.). You might want to include stamps for a large mailing list and perhaps money for envelopes and photocopying.
3. Please duplicate the enclosed materials (including the instructions and contact lists themselves) and distribute to all those on the contact list.

You should also include, within the inner sealed envelope, an explanation to those on the contact list specifying in a completely

generic way why you have taken these extraordinary steps, and why you need their help. Add any notes or comments you have that may help them to place the correct significance and importance on the material provided.

Another tactic I have also used is to provide the information on a diskette, rather than on paper. When doing this, I suggest that an opportunity exists for even greater protection of the information—particularly suitable for very sensitive matters. Create your files and then use file-splitter utilities to break them into A and B parts. Put A parts on one set of disks and B parts on another set. Put copies of the utility which joins the parts together on both sets so that, if a person has both, they can be reassembled and read.

Mail these out so that recipients receive only one disk—and are therefore unable to read the material themselves. But those on the internal mailing lists will receive multiple copies of both parts from many of those they had been distributed to. Not only do the multiple copies from several individuals strengthen the credibility of the material sent to the media, police, etc., but it also ensures A and B copies will be received. Nowadays, it is possible to convert audio or video material to computer data suitable for disk reproduction—though such will likely require many conventional floppy disks or some other removable media with larger memory capacities, such as Syquest™ or Zip™ cartridges. CD burners are becoming relatively inexpensive, too, so you can burn your own CDs with up to 600 MB of information—the equivalent of more than an hour's worth of compressed video data.

Of course, such an insurance policy means nothing unless you tell your opponents about its existence. This will probably be easy if you're certain you are being bugged; just tell them by talking to the wall. Sometimes, I call myself on a second line, and leave messages for them to overhear as I chat. If you are less certain about electronic eavesdropping, you can write them a letter. I like the latter. I prefer to make it generic and leave it anonymous. This makes them think twice on any similar ventures they may be engaged in—slowing them down at least until they can determine who sent it (they will, though you might want to ensure that eventuality with subtle clues). I back this up by leaving copies of the letter where they can find it. That way, they ultimately know for certain to leave me unharmed. Actually deliver it if you think that better. All this may seem like a lot of effort, and it is, but it really does work.

Doublespeak

Whether by telephone, writing, or face-to-face contact, there are often times when one side or the other will wish to communicate. Quite often, one party or the other will feel that the information to be discussed must avoid open mention or admission of key facts, names, etc. You must, then, learn the art of saying what you mean with allegory and double meaning, that only those involved might understand.

If you are confronted with a party who initiates doublespeak, it is better to play along than to confront the person with demands to speak plainly, for doing so may serve to frighten them off or inhibit their candor. If they are so uncomfortable with the topic to incorporate doublespeak, it is likely they will not wish to continue under any other circumstance. As an example, I needed to consult with an intelligence operative by telephone about some materials I had caused to be sent to him. In theory, at least, he and I were the only ones who knew the precise nature of the material or even that it had changed hands—but we both understood that my phones were monitored by my opponents. It was assumed that whomever was listening in was aware of his identity and would be interested in what we had to say. How do you communicate usefully without revealing your full hand?

In his first sentence, my contact provided me with clues to get what he was really saying and also gave me an "in" to join the conversation appropriately. Along with the rest of my material, I had enclosed some background material on myself, including literature on my foreign-investor services, and he wisely elected to use that as the basis for his doublespeak. "I received your investment portfolio and found it very interesting. It is very similar to other offers we have received in the past. I wonder if I could ask you a few questions?"

By this, I knew my information had reached him and that it was similar to information already in his possession—he was interested in pursuing the matter further. It also told me how to respond. "Well, certainly. In light of some of the significant financial risks the project represents, I can see that you would have questions. I myself have concerns about the feasibility study and the return on investment..." This told him that I understood his doublespeak and that I felt there were personal dangers involved, that I worried if he felt he could undertake the project and if he thought it would be worth his while.

The conversation continued at length in this manner. Anyone listening would have to be very careful about deducing the exact meaning of the conversation. In the end, they would need to take the broadest and most fail-safe interpretation and cover as many bases as possible, but none of them would necessarily be correct. It forces the enemy well off-center while allowing you to become better centered. The whole technique of doublespeak can be particularly useful to a covert operator, such as a spy, who protects himself through the use of plausible denial. If anything goes wrong, he has an innocent-sounding, plausible explanation for what happened or what was said. Play along. It's fun...

Footsteps Behind You

It is uncommon to be followed on foot. These days, a stationary or mobile observation post, perhaps augmented with audio or video systems, can accomplish a lot. A typical method involves two operatives who back each other up. Generally, they will try to position themselves well away from you, rather than close in—though I have had as many as three of them within fifteen feet of me at a given time. This would normally be an "arrest" mode of operation for law enforcement. They will flank you so that no matter which way you travel, you will not increase your distance from them. Listening in is not usually their primary agenda, though they probably won't turn down an opportunity to do so.

A private detective will generally be alone. Seeing the same mug for a good period of time about half a block back on the far side of the street is a clue. Always watch for the same faces, and watch the clothing too—though reversible outer garments, wigs, and other quick-change effects can be applied to confuse you. If you do blow these guys off, they could incorporate tag teams. Tag teams are harder to spot because they hand off duty to other members on a frequent basis. If you're dealing with federal folks, they might have a dozen or more people at their disposal. You have to learn to really look at people and find ways to remember them, and you have to learn to do it with what appear to be casual glances. Don't simply look directly at someone; it's a dead giveaway. When you catch someone watching you close in, just smile and say hello. It's probably not the bad guy, but even if it is, be friendly. Don't dwell on the contact. Act as if it was perfectly normal. When you see them at distance looking your way, check them again later. If

they quickly look away, that can be an indication. The real pros will not look directly at you and will not look away quickly but will opt to turn their head slowly, as if scanning the horizon.

How you look at them is important. When sitting at a table on an upper level, I find looking down through a drinking cup is effective. Raising a cup to drink from obscures your face, allowing you to glance sideways. Use reflections in plastic, glass, and metal to your advantage. If you must look directly their way, focus on a person or object near your target. Be aware if the target is looking your way or not. When you see they are not, you can get a good look at them for memory's sake.

You may wish to turn the tables. If you think you are dealing with a lone operative, go somewhere they are not likely to follow but that has a back avenue of escape, then come back around to where you can observe them from the other side. Wait until they decide to end their vigil, and follow them to their vehicle and beyond to find out who they are and who they work for. Or, once you have established some identity and perhaps documented it with witnesses or film, piss the guy off. Make yourself conspicuous watching him. After doing it for a moment, disappear, and reappear somewhere else. As he turns, let him find you standing there, watching him. They hate that! Take their picture. They really hate that!

The Rear-View Mirror

We have already discussed some aspects of vehicular tails. The thing to watch for, just as discussed previously regarding people on foot, are repeat sightings of the same vehicle. In a large city, you shouldn't see the same truck at different times and places on different days. Of course, you shouldn't confuse this with seeing the same truck on the way to work every day. The cops and feds usually have special communications aerials mounted on their cars. Some I describe as "rat tails"—little 8" to 12" black rubber antennas about as big around as a pinkie. Others I call "pig tails"—also short but made of black wire with little spirals towards the top. These are typically used with mobile telephone systems. Both of these are popular with local law enforcement but are also used by civilians.

Bigger aerials, or "whips," are usually black or white and can be so tall that they must be mounted low on a bumper, and even then, they extend several feet into the air. This type of aerial is strictly

for radio use. The various lengths of aerials have to do with the operating frequency range of the radio. If you see a truck with three or four such aerials of different lengths, you have likely run into a mobile command center—a valuable find. They are usually federal and up to no good—the different lengths monitoring police as well as their own Clandestine Involved Activities. These vehicles are also often used to monitor cellular communications or track vehicles that they have electronically bugged.

A car so equipped, perhaps with only two or three antennas, is likely a federal or local cop of some sort. If you see a marked police car with more than three, it is likely the Chief of Police, or a very high-level staff car, though more and more, this kind of equipment is finding its way into regular patrol cars in better-funded communities.

Again, a lone vehicle that stubbornly clings to you is more likely to be a private detective or an amateur—perhaps a stalker. An escalation to multiple vehicles means cops, at least. Continual replacement of vehicles and drivers and a wide diversity of equipment suggests federal agents, especially if they use commercial vehicles. On cabs and other commercial vehicles, watch for the vehicle number painted on the fender or body work; otherwise, they'll all look familiar. Aircraft, like undetected bumper-beeper tracking devices, are almost impossible to evade unless you can do a concealed vehicle switch.

Airborne Eyes

If your enemy has deep pockets, you can bet they've got aircraft. Law enforcement, particularly the federal kind, relies heavily on it. You can expect the same from any spies in the game, too. In my own adventures, I've noted the same aircraft buzzing low over both my home and my work on several consecutive days. There are simple, inexpensive solutions you can use to detect aircraft while you drive, such as purchasing the stick-on, bubble mirrors used to broaden your field of view of your rear-view mirror.

You may need to get inventive in order to adapt the device to your external side-mounted rear-view mirror at an upward angle of about 45 degrees. I used a large alligator clip, which worked fine. Cutting a notch in the underside one of the pincer handles allowed me to bend it downward at the end. A drop of superglue attached the mirror. I was then able to attach the device to the mirror's

housing at any time while driving and check the sky with a glance. Don't make it a permanent attachment, because your enemy and others will see the strange contraption and either figure out your method or think you mad.

Your first use would be to simply hold it out of the window and check. You will need to find a spot which lets you see over the roof of the car to the passenger side—where most pilots would elect to follow in parallel course. It is, after all, your blind spot. To see that part of the sky behind and to your right, you will need to hold the mirror out high and left of your own side window, or high and in front of the support pillar of your front window, or simply inside the car as far as you can reach towards the right-side window—which should be down for best view. The size and shape of your car's roof line and location of window pillars will determine which method, if any, works best.

I was often rewarded by use of this device—though the aircraft would appear too distant and too small to identify. An aircraft not flying parallel to your direction of travel should not be immediately dismissed. Watch to see if it zig-zags or circles over the roadway behind you, still generally progressing in your direction and maintaining its distance. The solution is to pull over for gas or to the side of the road and pretend to check a tire or pop the hood momentarily. Sneak a glance as the aircraft is at its nearest point.

If you can get a tail number, contact the Federal Aviation Administration to find out who owns the aircraft. Knowing who the owner is may not tell you much because the aircraft may be rented or leased to other parties, but it's worth a shot. Naturally, you will need to take care to avoid giving away your identity and the true nature of your inquiry. I suggest you say you want to complain to the pilot for flying too low a populated space. If the owner does not want to cooperate, tell him you will go to the FAA with your complaint, and he can deal with them. He probably won't want to have that happen; if he still refuses to divulge pilot or user information, he is likely part of the effort against you. You should then check more into his background and affiliations.

Postage Due

Mail tampering is something which you might experience, especially if you're dealing with unscrupulous or federal enemies. If you do have this problem, it is likely to happen with both inbound and

outbound mail. When this happened to me, 80 percent of my mail either arrived very late or was waylaid entirely. Sometimes there was direct evidence of tampering, such as being sent as an empty envelope ripped open at the seal. Worse, almost all of my business mail was tampered with in a way that denied me income and angered my clients. My business went from perhaps ten orders a week to zero, and old clients began asking for refunds for the shoddy service.

After that, I generally mailed things I wanted the other side to see. I would test to see what materials or information would be censored or get a reaction. If you need to mail something with any certainty of it getting to its destination tamper-free, use wide, heavy-duty rolls of transparent sealing tape. Use an envelope made of soft paper—paper which tears easy and that seems sort of fuzzy compared to a tight paper which is hard and smooth. You want the paper to tear easily and, more importantly, to come apart when tape or a gummed sealing flap is applied and removed/opened. After sealing your envelope or parcel in a regular fashion, stretch out a length long enough to run the full width, and beyond, of the mailed piece. Use a permanent marker to initial the sticky side of the tape. Use this tape to seal the package over the label and primary seal, wrapping the excess around to the other side. There should be no way to open the item without either removing the tape or tearing the wrapper.

Write in large letters "photocopy prior to opening," and photocopy it yourself before sending. Arrange with the recipient to photocopy it and fax the copy back to you upon receipt. If the two copies do not match, you know the material was compromised. This approach works best when the material is something which you do not mind losing and which is not overly harmful to you if compromised—that's how the text for this book was transmitted to the publisher. The final step is simply to send it in some form of registered mail. You might want to insure it to provide even tighter controls. One nice thing about this method is that, if it does arrive in a different form, you now have evidence and can approach the postmaster or other appropriate authority for investigation.

When you need to be absolutely sure the material you are sending arrives intact, there is another approach. Send it via regular mail, unobserved, if possible. Use a wrong return address, and disguise your handwriting. Don't mail it to the party you wish it to go to, instead, put the item inside another package, and mail it to a

cab service in the same city as your target. Include a cashier's check and a note asking the cab company to deliver the post for you. I have found that this works very well. A similar ploy is to find the address next to your party, and if you're certain they aren't bad guys and that they know the target party by name, use the right name but the wrong address—they will pass the mail along.

Stakeouts

Any place you frequent could be under some form of observation. It might be from a nearby house or apartment or a nearby office. It could be a motor home or a van. Any location or vehicle near you that affords a good view, with no obstructions, is a candidate. In choosing a site, your opponent will consider a site that affords a good view of the main entrance. A good position allows for viewing of alternate access ways, such as a back alley. A second observation point may be called for. Keep in mind that vans can be equipped with periscopes that peer out of roof-mount air vents or other openings.

Think about what buildings around you have been recently available for rent or lease. If a vacant apartment for rent is suspected, you might have a friend make an appointment to look at it. If he can't get in, or if anyone is seen clearing out before—and returning after—the appointment, you may have located a post. Your neighbor could be harboring a post. If you can access night-vision gear, have a friend study the site from a safe point—a trick that has worked for me.

If the site is vacant, consider this little ploy. Have a friend "prowl" the site. Call 911 and tell them you are investigating it, and give a description of your clothing. They will tell you not to do this, but tell them you will anyway, and hang up. Grab a baseball bat and hot foot it on over. Depending on your bravado, and the availability of access, you may choose to enter the building. Breaking a window or a lock may not be a good idea, but you can always claim you heard someone doing just that and found it broken when you arrived. If you don't want to go in, just tell the cops you heard someone inside. Let them check on it for you. The 911 response team will not likely know about the post, even if there are cops manning it.

Before you take any of these measures, you might want to decide how much you care that you're being observed. As strange

as it sounds, it may work to your advantage to have them watch you rather than blow their cover and force them to go away. This is also true for other forms of surveillance. There are no hard and fast rules—its just a matter of whether you can find ways to use their surveillance as a tool to disinform and manipulate them. And if you are able to work around it, say, if you have found a way to sneak in and out undetected, then you have a definite advantage you might want to hold on to.

LISTENING IN

Electronic eavesdropping is a significant invasion of your privacy that, in many cases, is easily accomplished. Many of the techniques are difficult to detect, while some are rather easy to spot. Detection and isolation may require specialized equipment and expertise and can be rather expensive, but this is not always the case. Some methods are legal with the proper warrant, others are violations of the Constitution or of local or federal laws. In theory, at least, obtaining a warrant for this is difficult for all but the most severe cases.

One method of eavesdropping is perfectly legal. Any sound which escapes your home or office, or which is otherwise made public, can be accessed at will by anyone, and there is nothing you can do about it but to stop making the sounds or intercept them before they get far enough to be heard. This includes the use of cordless telephones, walkie talkies, intercom systems, or any other radio-based communication system except cellular phones. Conversations which take place via cellular phone are protected by law, but people still listen in on them. Many of these people are just electronics enthusiasts and thrill seekers. The point is, don't use radio frequency–based devices if you want your conversations to remain private. Even a so-called "scrambled" cordless phone message can be easily listened to by those with a desire to do so. But we are not limited to discussing radio devices here. I'll cover all these in greater depth later.

Shotgun microphones and parabolic microphones are highly directional and can be useful for selectively amplifying sounds at great distances. Lasers can be modulated and bounced off of a window from more than a mile away. The reflected beam will, by virtue of interference in the modulation caused by the vibrations of the window, contain a very accurate and usable record of what was said within.

For these systems to work, the listener must be in a line-of-sight position relative to the target. For the laser beam, the line of sight must be perpendicular to the window, as the light beam must be reflected directly back to the transmission point—though advanced versions reportedly work on diffraction principles not unlike laser radar and can therefore be placed at any angle to the target. If you suspect this form of listening, you will likely be able to determine where the listening post is, since if they can see you,

you can see them. Of course, you may need binoculars to do it.

Another problem with lasers is that they generally operate in the visible light spectrum—you can see them. About 50 percent of the light or better should be reflected by the window, but the rest should produce a spot somewhere beyond the window. Usually, they are aimed at something just inside the window which cannot be seen from inside, such as a curtain or blind, or at something which in some way conceals the spot, such as a flower pot or fireplace opening. Use a white sheet of paper to pass over the entire surface of a suspect window and see if you can observe a small (typically 1/8th of an inch or smaller) red or orange dot shinning through.

There are a couple of approaches you can try in order to defeat these systems, but there is no guarantee. Speaking in whispers, for instance, might not deter a sensitive, professional system. Placing a radio against your window can help, but again, a good system might be able to overcome it. Computers can be used to filter out such interference, but only the advanced players will likely have that tool. The best deterrence is to shut down sensitive discussions anywhere near suspected windows.

A technology that predates the laser is still the preferred method of attack for most parties. It is called the "bug", a microphone/radio transmitter. Appendix IV, at the end of the book, contains extensive information on the bug and its detection. We will simply discuss a few points on strategy here.

It used to be that bugs were relatively large and easy to find with just a careful visual inspection. Nowadays, a good bug can be so small it can be concealed in the crack of a floor or underneath a chip of paint on the wall. It can be made to look like a normal object such as a pin in a pincushion or a nail in the wall holding up a painting. It takes an expert and expensive gadgets to locate them today, unless it is of the most unsophisticated kind such as might be used by an amateur who grabs whatever he has at hand and simply relies on a clever hiding spot.

But there are a few questions to ask before even looking for a bug. What will you do if you find one? Do you really want to eliminate it? If you do, your opponents will realize your awareness, and you will lose any ability to feed them disinformation. You must weigh your options. Bugs are not easily traceable, but with one in hand, the authorities may have more to go on. At the same time, you might have more to gain by keeping it in use. In the end, it

may be better to simply document the existence of a bug and leave it in place.

Bugs need to be serviced from time to time in many cases. They require their batteries to be changed and their aim fine-tuned. This gives you a chance to catch your opponents in the act or to follow them. The only drawback is knowing that everything you do or say is being listened to. This psychological issue is addressed elsewhere in this work. It can help to take a cavalier approach, and let it be known that you "think" the bugs are there but that you can't find them and are just living with it. You can then talk to the walls whenever you wish to address the other side, and act like you are trying to conceal things. Whisper—they can still hear it. If you truly wish to communicate without them hearing, use paper and pen.

One other fun aspect of leaving bugs is place is that you can engage in your own psychological warfare against your enemy. Because they must listen to EVERYTHING that goes on, usually via multiple microphones in rooms about the house, you can use this to express your humanity and patriotism in ways that wear down their resolve. You can also just plain irritate them. Tune your radios and televisions to annoying and conflicting stations while you don headphones and listen to your favorite stereo tracks. They get country-western blended with talk-show dialog, foreign-language programming, and classical music—a mix guaranteed to make anyone twitch. The amusing thing is, they have to listen extra carefully, because this is just the sort of thing someone would do to conceal sounds they didn't want picked up. You can reinforce that notion further by then engaging in harmless "secret" dialog.

Another fun trick is to remember that actions you take make sounds. I like to tinker with my furnace, making all the sheet metal boom. Conclude with something like, "Find that, if you can..." The times when I have done this, I found through my use of indicators that upon their next entry, the spies took great interest in the furnace. If you can think up ways to make sounds that are hard to figure, so much the better. Be devilish ... and do have fun, please!

Multiband Radio Scanner

A scanner will naturally let you listen in to police radio traffic. Even if your opponents are not law enforcement, you might find this useful. A scanner can also let you hear walkie-talkie or car radio conversations. My wife came home one night to hear some-

one using walkie-talkies in our basement. The men fled without harming her, their mission being to secure copies of documents kept at the house. If she had been using a scanner, their conversations might have tipped her in advance, and she could have gone to the police. Note that I did not say call the police. Our opponents would also have scanners and would immediately pull out as soon as a radio dispatch was issued. By going to the police, she could arrange for a surprise raid.

Cellular Phone

Cellular phones automatically and frequently change working frequencies to the strongest signal available from the many cellular radio service broadcasting towers in the area. This is especially true when in motion. When using a cellular phone, you can hear a soft clicking when the frequencies change. With some experimentation, you can usually find a place where simply walking back and forth around the corner of a large building causes repeated switching. Because there are literally thousands of possible frequencies and the phone may change frequency several times a second, you can make it almost impossible to eavesdrop on your cellular communications.

The best cellular phone is one which is not digital. Many people, myself included, believe that one of the reasons the industry is going digital is that such systems will make eavesdropping by the government easier. This is possible because of encoding of frequency-switching functions within the data transmission packet, making it easy for high-tech listeners to automatically switch listening frequencies as quickly as the user's phone. The whole digital communications net was designed with help and influence from the NSA, which is the CIA's big brother. Disregard the sales hype and get an older phone. For even better results, urge those you expect to call regularly to use a cellular, as well. Cellular-to-cellular communications, especially when both are mobile, are very difficult to monitor. A warning, however. Never let your phone out of your personal control. It can be "borrowed", modified to be "listener friendly," and returned before you notice....

As a final warning, do not leave your cell phone on standby mode as you travel. Cell phones continually broadcast identification information which can be used to track you down. The only

safe cell phone is one that is turned on only when necessary. The same is true for pagers. The very reason you have these things becomes the very reason they work against you. Thus, in order to use them properly, you need to alter your lifestyle with respect to their use.

Computer Security

No system is absolutely secure from threat, and there are several areas of concern and several tools with which to combat the problem. Anyone who can gain physical access can probably get at the data on the hard drive in one form or another. You can kill the power on the computer's circuit and lock the breaker panel. This is not always practical, and can still be defeated with extension cords, portable uninterruptible power supplies (which you might already have installed anyway), or breaking the lock.

Some computers have or can be modified with a locking power switch as a second line of defense. However, anyone with a screwdriver can disassemble the case and short past the terminals of the switch, or as is the case with most locks, they are so simple that a novice can pick them. If you elect to use this method, I suggest installing a lock with a mechanical restraint within the case to prevent disassembly even with all screws removed.

There are a number of software and hardware defenses which can be used to protect the information in your computer. You can install utilities which automatically open when the computer starts up, asking the user for proper password clearance before allowing access to the computer. Likewise, there are other lines of defense which offer file encryption with password-equivalent decoding requirements in order to access individual files.

Unfortunately, there are ways to defeat all of these, though it will be unlikely that any but the most sophisticated and well-resourced opponents will be able to do so. It is possible, for instance, to force the computer to start up from a floppy disk instead of its native hard drive. Once this is accomplished, the user has full access to the system. Given enough time and knowledge, virtually any data encryption scheme can be defeated by a good opponent.

Password-based systems store the password on the computer's hard drive for comparison. A good hacker will know how to find it by using special utilities designed to snoop out the password at the binary level. Therefore, encryption is better, as it does not store

the decryption code on the disk anywhere. Rather, it simply applies the user's input to a complex binary manipulation of the data. When the file is originally encrypted, the data is scrambled and stored in that form. Only the correct user input will properly decode the document.

However, there is still a problem if you are dealing with federal agents. The NSA once more is at the heart of this particular villainy, having established a standard for encryption software. What most people do not know is that the NSA standard was deliberately set such that NSA decryption software can easily crack the code by using their state-of-the-art supercomputers. I know this because I worked for a company which sold software to the NSA used in developing these decoding tools. All that is necessary is for the encrypted file to be copied over to some portable storage media. The NSA (or NSA on behalf of CIA, DIA, FBI, etc.) can then decode the encrypted files at their leisure—generally in less than an hour of computer time.

The only sure way to keep your information safe from snoops may be to not keep sensitive files on your computer. This means that you should store important files on removable storage media such as floppy, Jaz™ or Zip™ disks (or older media such as Bernoulli cartridges), various optical systems, or tape backup systems. Then, of course, you only have the problem of how to keep these precious targets secure. Do you put them in a hiding place where they might be discovered? Do you put them in a safe deposit box where they might be illegally accessed by warrant, fraud, or trickery? Do you keep them on your person, where they might be taken forcibly?

Consider all of these options. By creating multiple layers of defense, you can often at least detect if someone is tampering with your system or attempting access. This gives you the opportunity to take extraordinary precautions which can set them back to square one—such as changing all the locks entrances to the building, changing filenames, passwords, encryption methods, storage methods, etc.

Unless you have an ISDN or Web TV for Internet access, you'll be using a standard telephone to transmit information, and you are subject to all of the normal telephone eavesdropping techniques. However, there are good tools to protect computer transmissions. Before calling up the destination computer, encrypt the file first with your best encryption software. But this alone is not enough.

Get outdated encryption software, and use that, too. Any file so transmitted is effectively encrypted twice. Even NSA methods, no matter how advanced, should not be able to crack this protection because even if successful in finding the outer level of encryption, the data would still look encrypted—the software would not know it had "hit" and would continue looking for the right combination.

The catch is that the person receiving your communication would need to use identical software and know both encryption passwords. This can often create a security problem for obvious reasons. Not only must you be certain that you can trust the other party but you must also find a way of communicating passwords safely. This is not always easy, especially if you must create or alter them with short notice or you do not have personal contact with the party. This means you must devise a means of communicating passwords which is secure from mail tampering, telephone wiretaps, or surveillance pitfalls.

I quote from "Infowar Imperils the Security of Computer Systems," a Knight-Ridder News Service article by Reid Kanaley that appeared in many newspapers nationwide. I found it in the April 20 edition of the *Oregonian*. The lead for the article, which seems aimed at espousing more Draconian measures to ensure Internet security, begins: "If they are connected to the Internet, they are vulnerable to hackers, thieves, spies and information terrorists." How very appropriate to our discussion. Then there is this: "I know a lot of banks who say, 'We are impenetrable,' and they are wrong," said Winn Schwartau, who maintains that his consulting firm, Interpact, Inc. (www.infowar.com), has failed only twice in 2,300 attempts to penetrate his clients' networks.

Schwartau, who coined the term "Infowar" in a book he wrote in 1994, says in the article that his clients even include the Federal Reserve. Schwartau, incidentally, is also an expert at using TEMPEST technology to read what you are typing on your keyboard from a van down the street—discussed elsewhere in this work.

The article also cites programmer Dan Farmer, who "conducted a study to see how easy it would be to break into various sites on the World Wide Web..." He found "the rate of successful attacks on Defense Department computers was no different than at other Web sites. 'I barely electronically breathed on these hosts,' Farmer reported of his survey of the Web-hosting computers of organizations that included banks, federal institutions and newspapers. 'Over 60 percent could be broken into or destroyed.'" I close my

review of Interpact, Inc., to include the fact that personnel associated with that firm were involved in public verbal cyber attacks against the investigation into possible friendly-fire involvement in Flight 800. Through Ron Lewis, a former military intelligence member who seemed very cozy with assorted "infowar" experts, including Interpact's own, threats were lobbed at select proponents of the friendly-fire theory. Shortly after these attacks and threats, the lead proponent of friendly fire found he could no longer access his own Web site and e-mail. Somone hacked his ISP and planted a "bot" (a robot-like software routine) which continually altered his password. Interpact, and for the matter, the Internic (the folks who literally control Internet access for ISPs and domain names) are both thought by a long list of fellow paranoids to be fronts of the intelligence community. This suggests that the whole of the Internet system has already been or will soon be subverted into a network of ready information access for Big Brother.

As far as Internet security is concerned, consider the fact that Macintosh-based ISP (Internet Service Providers) are by far much more secure than PC-based (IBM clone) ISPs. In fact, there are many instances where Mac ISP hosts have offered $10,000 rewards to anyone who could crack or hack their way into their system, rewards which have gone unclaimed for years. However, I know of no instance where any PC-based host has offered a reward (even as low as $2,500) that wasn't hacked within weeks of the offering. Even the CIA's own (PC-based) Web site was hacked recently, a matter I happen to know something about because a college professor whose students were apparently involved contacted me for help and advice because the CIA suspected he had something to do with it, too. For more information on this, visit my Web site at www.proparanoid.com.

Most people don't know that computers, fax machines, copiers, and laser printers have an Achilles heel. To the intelligence community, it is known as TEMPEST—Transient Electromagnetic Pulse Emanation Surveillance Technology. All digital electronic devices driven by microprocessors emit certain radio frequencies. Although they are very weak in strength, they can be detected and manipulated by anyone listening in with the right equipment. Again, thank the NSA for this clever eavesdropping tool. If the other side knows the hardware and the software you are using, they can interpret the RF emissions of your hardware to duplicate the material you type into your computer, copy with a copier or

fax machine, or print to a laser printer. In order to monitor such systems in this way, your opponents will need to be nearby and in a line-of-sight position. All they need is a closet or a van with portable equipment. As you type on the computer or operate the fax, copier, etc., everything is processed in real-time to appear on your antagonist's computer screen just as you see it.

You can thwart such attempts in several ways. First, attach all of your equipment to an uninterruptible power supply (UPS) to isolate the AC input. RF emissions can "ride" the current through induction in a way that is accessible by tying in to your wiring or by amplifying the broadcast of RF for traditional reception. A UPS uses a transformer which stops both possibilities cold. Note, however, that UPS units are often targets for hiding bugs, so ensure that these are protected in some way which allows you to determine if they have been tampered with, such as painting the screws and photographing the unique result.

Second, if possible, wrap your computer or other device in chicken wire. This should not come in contact with the screws or other metal parts (you can layer the wire with cloth or some other insulator at appropriate contact points). The chicken wire acts as an antenna to catch the RF emissions, and if you ground the chicken wire to earth, the signal goes no further. This is often called a Faraday cage.

Some people claim this works, others say it simply acts as an antenna. No engineer types I have talked with have expressed any concerns at its usefulness, except that the ground should itself be to earth, not to your common electrical system ground. An AC ground method can force AC carrier pickup of your RF. A direct earth ground is achieved by running a heavy copper wire directly to a metal stake driven approximately three feet into the earth. An alternative is to connect the wire directly to plumbing. Use caution with either method, however, because if your opponents can tap the wire or the plumbing, they may be able to pick up the RF directly. I suggest a secure, internally run wire which you can either visually inspect frequently for integrity, or one that is not accessible at all.

The later technique works well when it can be built into a facility. You can then embed the chicken wire within the walls, floor, and ceiling of the computer room. Experts advise to build the walls out of solid concrete or filled concrete block. This achieves the same RF stopping effect and secures all equipment in the room

without individual treatment. Indeed, it might be worth doing the entire structure in this way.

More Exotic Surveillance

The intelligence community is known to have a rather interesting arsenal of devices at their disposal. This includes devices able to see through walls, devices ranging from spy satellite systems to helicopter-mounted Forward Looking Infrared Radar (FLIR) systems to much smaller systems using millimeter wave technology. Consider how the following device might be used against you by an observer who might have access to the technology and a desire to know exactly what you are up to, but who does not have the ability to place a camera in your location. The material offered here comes directly from the Web site of VSE Corporation, a company making a device described as the Life Assessment Detector System (LADS), and the Web site of Georgia Tech.

LADS

The photographs of LADS equipment provided at the VSE site seem unusually dark and deliberately silhouetted, and this makes it difficult to read the material on the electronic boxes. Despite this, one of the connectors clearly seems to be a video connector, suggesting the equipment can generate a picture, something implied by the text description of its function. Attempts to gain more information from the manufacturer have gone unanswered as of this writing. Within weeks of inquiring, this material, and this material only, was removed from their rather large site (www.vsecorp.com).

The Life Assessment Detector System is described as a "microwave Doppler movement measuring device" and appears to spring from the work of Eugene F. Greneker at Georgia Tech. It can detect body-surface motion, including heartbeat and respiration, at ranges up to 135 feet. LADS is actually a 10 GHz x-band continuous wave microwave transceiver with a nominal output power of 15 milliwatts. It uses what is described as a neural network to store a variety of complex patterns such as visual waveforms and speech templates, and it compares sensor readings to previously stored patterns. The description suggests that it can be trained to recognize specific individuals and, thus, to track their

movements within a building—though they certainly do not address such an application.

LADS is claimed to be developed to detect people who may be trapped in building rubble; battlefield casualties in a chemical/biological warfare environment; victims of airline, train, or automobile crashes, avalanches or mudslides; and hostages. For more information about the LADS, e-mail info@vsecorp.com. Perhaps they will answer you.

There is another example of the LADS technology that seems more to the point—a Radar Flashlight that sees through walls, as described in a press release and paper from the University of Georgia Research Institute (www.ga.edu). It is about the size and shape of a large flashlight, and an accompanying unit containing the electronics is about the size of a small portable radio or CD player. The radiation involved is claimed to be very small: ten times less than the voluntary exposure leakage level for microwave ovens in the United States.

Included is a photograph that simulates an actual, visual, see-it-through-the-wall application of the device, with the headline "Radar Flashlight Would Help Police or Corrections Personnel Detect Human Presence Through Walls & Doors." "Based on respiration signature alone, the Radar Flashlight allows us to detect a stationary individual behind a solid wooden door or standing four feet behind an 8-inch block wall," said Greneker. "These qualities make the flashlight potentially useful to police officers in ambush situations and to prison guards doing bed checks." Like LADS, the review goes on to describe applications for detecting injured parties in collapsed buildings and other medical or emergency uses and describes the Radar Flashlight as merely one of a family of technologies. The documents claim the first system of this type was developed in the mid 80s under the sponsorship of the United States Department of Defense.

The technology behind the LADS and the Radar Flashlight is shown to be tied to battlefield testing and includes tests conducted at the 1996 Olympics in Atlanta, where the subjects were archery and rifle competitors. According to the documents, it was envisioned that the demonstration would be of interest to the television networks covering these competitions. This seems a rather thinly veiled excuse for such tests. It is unclear if the competitors knew they were being monitored or not, or if permission had been given. One might presume that one reason for such testing was to

see if the system could detect changes in the heart and respiratory functions of a person about to fire a weapon and thus, be able to provide advanced warning.

The paper also confirms that the device can be trained to recognize a specific individual. "The technology's potential to monitor heartbeat raises some interesting possibilities," Greneker notes. "This version of the system might be used as a biometric identification tool," he said. For example, if it could be shown that an individual's radar heartbeat signature is stable over long periods of time and is unique to an individual, the remotely sensed heartbeat could serve as a fingerprint of sorts.

The prototype unit shown operates on a frequency near 10.525 GHz and is a homodyne radar configuration, although a frequency-modulated continuous wave (FM-CW) system could be used for applications where information is required to determine the range to the target. It is expected that the final version for law enforcement use would be under $500. Thus, this technology will likely be applied broadly (hopefully against criminals only) in the near future.

LADS and the Radar Flashlight are devices right out of *Star Trek*. You may remember the episode where an unauthorized alien presence was located on the ship by means of heartbeat monitoring, where every known crew member's heartbeat was eliminated from the ship-wide listening device, and the final remaining heartbeat could then be located precisely. This is what these current-day devices are capable of, were they to have in advance the needed data on a given person's heartbeat. Not exactly your typical picture-taking device.

In addition, millimeter wave devices exist that, according to James Atkinson and others, the intelligence community can use to see through walls—producing thermal images to reveal location and activity of individuals on the other side. You may recall the helicopter-mounted version in the film *Blue Thunder*. While that was a far-fetched action-adventure fantasy, virtually all the technology portrayed in the film does exist. Then, of course, there is remote viewing.

Remote viewing is controversial and thought by many to be a hoax. However, there are documented private and federal studies which give credence to the notion. Remote viewing is the ability of select individuals to be given a key bit of information about a person, place, or thing and then see the desired target and what is

going on around it. It is claimed that almost anyone can use remote viewing if properly trained, and there are schools claiming to train anyone. There is an abundance of material on remote viewing to be found on the Web.

Telephone Security and Electronic Surveillance

Anyone can become a target of electronic surveillance. There are many, many reasons any given individual or organization can become a target. The trick is to determine the reason and find evidence to support the conclusion that the deed has indeed been done. The following examples and reasons for being bugged and the telltale signs to look for have been stolen and edited, with permission, from the Web site of Granite Island Consulting (www.tscm.com), courtesy of James M. Atkinson.

Relatives bug each other. Businesses bug competitors. Employers and employees bug each other. Students bug professors. Insurance companies bug claimants. Attorneys bug each other. Salesmen bug client conversations. Collection agencies bug debtors. Law enforcement bugs suspects. Rock fans bug musicians. Private investigators bug everyone else for anyone else.

The chances of being bugged increase in certain situations: being involved in lawsuits; questioned, arrested, or arraigned by law enforcement; marriage, divorce, or separation; running for or being elected to any public office or promoted to any high public or business post; political activism; working for or applying to a defense contractor or government agency; working at a business undergoing tense labor relations or involved in litigation; a public corporation about to issue stock, consider a merger, or resist a takeover attempt; virtually any high-tech company, any firm engaged in research and development, patents, copyrights, and other trade secrets; simply being wealthy.

Here is a checklist of things to look out for if you suspect you are being watched: others know of professional or personal secrets of which only you should be aware. Your radio, television, or telephones have suddenly developed odd interference or signal irregularities (telephone noises, TVs turning themselves on or off without command or exhibiting picture defects such as herring-bone patterns, static, snow, ghosting, etc.). Your home, business, or cars have been broken into—perhaps with nothing taken. Electrical/cable/telephone wall outlet plates no longer match their

original position (paint/dust/discoloration lines don't match), or the paint seal on screw heads are broken (an indication that the screws have been turned). White debris or dust is found along baseboard areas (wallboard particles). Discolorations in wall paint or unusual bumps (typically the size of a small coin). Unusual frequency and prolonged stay of utility/contractor/delivery/ trucks near your home or business. Workers show up to do unscheduled work. Furniture or items moved or rummaged through. Computer files or media seem tampered with or sabotaged. This is by no means a complete list. The one I like best is when neighbors are able to listen in on your conversations with their radio.

Common Bugs

The following material, from Tim Johnson's Technical Surveillance Countermeasures Services Manual, gives insight to the susceptibility of your telephone to eavesdropping—not only of calls, but of any audible activity near the phone—even when you are not using the phone. "Assuming your telephone is operating properly when installed, there are a number of things which can be done in just a few minutes. The hook switch inside the phone can be attacked and bypassed through the simple task of bending the contacts so they are always touching. Resistors, diodes, and capacitors can then be installed across the hook switch. The mouthpiece can be replaced with another that is also a transmitter, connected to the incoming lines for power. This type of installation would be in operation at all times, not just when you are using the phone. Should the phone be permanently mounted to a desk or the wall, an induction coil could be hidden under or behind it. Going a step further, an induction device can be used on the telephone at any location between the point where the phone enters the wall and the main telephone plant. If the information is important enough to warrant the expenditure, you may be monitored by intercepting microwave signals or even satellite signals." Anywhere within the telephone system where the wires to your number are accessible, a bug can be placed. In modern systems, it is even possible to create a software bug that reroutes the signal to another destination.

Here is a brief summary of the most common bugs, compiled from information provided by James Atkinson.

RF Transmitter. This is a classic phone bug. A small RF transmitter is attached to your phone line. Power may be supplied by the current on the phone line or from a battery. Most devices of this nature only transmit when the phone is lifted off the switch.

RF Transmitter with Microphone. Similar to the above device, but it has its own microphone, and is typically installed inside the telephone. Normally considered a room bug. It may transmit the RF over the phone lines, as well (carrier current—9 kHz to 32 MHz typical).

Infinity Transmitter/Harmonica. An older device that was attached to a telephone. When called from an outside telephone, it would enable the caller to listen in on the room where the device was placed. Considered obsolete but still available.

Recorder Starter/Drop Out Relay. This is little more than a device that detects when you lift the receiver off of the hook. Its purpose is to activate a tape recorder hidden nearby. This type of device is popular with private investigators and "wannabe spies." Some recorder starter devices also detect sound, and only activate if sound is detected on the line.

Remote Observance Monitoring. Allows the phone company or government to legally tap/monitor your phone by sending a remote software command sequence. The computer that handles your calls is instructed to transmit a real-time digital copy of your call to anywhere in the world. All that is required is access to the ESS translation and access to a T-Carrier or OC-xx data line (a normal "loop" line is rarely used). With a 622 MB fiber-optic line, most users can easily access (record) over 11,100 lines at a time in a local area. This function of the phone system is very loosely controlled, as the maintenance people at the phone company use it for routine maintenance. Any computer hacker can easily access the system. Savvy private investigators and insurance companies have been known to use this method illegally to gather information.

Hook switch Bypass Methods. Inside your telephone is a switch that disconnects the microphone when you hang up. Your phone can be modified so that the microphone is on all the time. If the

microphone is hot all the time, the spy can go anywhere outside of the building, plug an amplifier into the line, and hear what's going on. It is effectively the same as installing a microphone in the room.

Simple Bug Detection on Phones

You may be able to locate telephone bugs without expensive equipment or professional aid—though a professional will advise you not to attempt it. Note that the procedures offered here are not foolproof. You also run the risk of letting the other side know that you are on to them, and they may simply take evasive action. I have not personally tested the methods I am about to relay, this is simply information I have compiled over the years. This author and the publisher warn that you perform these tests at your own risk, and there are no guarantees of performance or safety. However, they have been reviewed by those familiar with phone systems as technically feasible and safe, provided reasonable care is taken with respect to voltage versus signal lines.

Testing your phones for common bugs will require a VOM multimeter with high impedance scales (a digital unit with FET circuitry is preferred). You will also need an expendable telephone cord, wire strippers, and a set of screwdrivers. Get a phone you know to be bug-free, say, from a flea market. This will be your test phone.

1. Preparations. Remove the face plate of a wall jack and observe the wire colors. You will need to know which leads of the jack mate with which color telephone wire and which wires are not used at all. Cut the end off of your expendable telephone cord, separate the individual wires about six inches down, and strip them.
2. Isolate your phone system, and test the voltage. Disconnect the phone line where it enters the building. Measure the line voltage at red and black (ground) leads. It should read 48 volts. If you notice variations in voltage, you may have a wire tap. Note that the current will "tingle" if you short yourself to ground while holding the hot lead, but the amperage is so low, there is no danger.
3. Test your phone wiring, part I. Disconnect all phones. Set the resistance scale on your multimeter to a high reading, and measure resistance on the line using various

wire pairs (recall step one, where you noted wires in use/disuse). Try all combinations of in-use wires in pairs. It should be very high on the order of a million ohms or more, since you are measuring the resistance of an open circuit. If it is significantly less, there may be a listening device on the line. This usually causes a reading in the 50-100 kΩ range. Follow the cable run to locate it, since it will likely be installed where access is reasonably good. It might even be right in the wall outlet.

4. Test your phone wiring, part II. Twist the ends of disconnected wire pairs together. Go to the other end, and measure across the pair at the open end of the makeshift circuit. If more than one or two ohms, you probably have a series bug or a dropout relay, used to trigger tape recorders. Note that larger facilities that have dozens of phones will likely read this high under normal circumstances. Look for readings commensurate with the increase in wiring volume. Again, test all pairs in use in every combination. Again, trace the cable run, this time looking for a point where there is a break in the wire which might allow an object to be inserted between the ends of the break. It may simply look like a wire splice with black electrical tape wrapped around it.
5. Test your phones. Hook up your test phone, return to the other end of the line, and untwist the pairs. Read the resistance on each wire and note it. This represents a normal, clean phone. Replace this phone, one at a time, with the other phones removed earlier from your system, and test them as well, comparing readings. Where resistance is notably higher, you may have a phone with some kind of bug in place within the unit itself. You may or may not be able to detect the unit by examination, depending on sophistication.
6. Optional test of phone line to "pole." If you are brave, and are certain that you are not under visual observation, you may elect to climb the pole or trace your telephone feed to the main underground/above ground trunk box. On the assumption you will be dealing with a junction box serving many clients, and no posted list of numbers exists (look for small hand-

written numbers beneath each set or a "map" of numbers on the panel door—this is uncommon, but you can get lucky), apply a small voltage, such as from a penlight battery, between any two disconnected lines coming into the building at the phone end. Note the color coding of the selected wires. Use the VOM to find the hot leads of the same color coding at the panel on the pole or box. This will identify the set of leads to your facility. Each set of leads from the building should go to the panel and terminate there, or they might have an additional set of wires for each leading out. In the latter case, if yours is the only one that has extra wires, you have found a physical tap. Note where these seem to lead, if possible, in hopes of determining where the listening post is located, likely a neighboring building. They will likely go to some other phone block, one which is likely not connected to Ma Bell via any means other than your wires. This will be apparent if there are no inbound wires like those going to your terminal set.

7. Optional Identification of Listening Post (from step 6). Under the old Ma Bell phone system, every city had a DPAC office dedicated to assigning numbers to the telephone wire pairs on the poles/underground/aboveground boxes, which are used by telephone linemen and service reps installing/repairing phone systems. If you have a DPAC phone number, you can locate a twisted pair combination by telephone number, street address, or you can get that information based on the wire pair info (those preprinted identification numbers on the terminals themselves). You may also need the pole or box number, which should be somewhere on the unit. It takes a little courage and the cavalier confidence of someone doing the same old thing day in, day out. If you think you can't master that deceit, pretend it's your first day on the job, and say so, being deliberately clumsy, perhaps.

To get the DPAC number, call the regular customer service number for billing information, and ask for the DPAC number as a telephone insider from a neighboring community. You might say

something like, "Hello, Portland, this is Harry from the Salem business office. I need your DPAC number for the southeast." There should be no difficulty, but if the person is not helpful or does not know the number, try locating a different customer service number, or just try again later.

Then call the DPAC number thus obtained. "Hi, DPAC, this is Joe from the Salem Phone Store, I need the telephone listing for 812 First Street..."; "...address for terminal pairs ##, and ##..."; "...terminal pair numbers for 812 First Street..."; "...phone number for terminal pairs ##, and ##." You get the idea. They should again provide you with the information requested, even if the number is unlisted. You can apply this trick in other situations, obviously.

If you're worried about caller ID, use a pay phone or a friend's phone. Tell them that, if anyone asks, they can say someone claiming to work for the phone company asked to use the phone. Of course, under the new digital phone system, there are no local service center phone numbers, and in many locations, there may no longer be a DPAC center. You may need to improvise over several phone calls to determine exactly who to call and what to say or ask for.

Telephone Harassment

Sometimes your opponent may elect to apply your own telephone as a weapon against you. What follows is advice that can be handy for any kind of crank-call situation, regardless of whether it's just some kid having some fun at your expense or part of a larger problem.

Your phone is your use, and for your use only. You pay for it, so you get to decide when and how you use it. I sometimes deliberately let the darn thing ring till it stops, just so I'm not a slave to it—to reinforce the notion that I own it, not the other way around. I know that sounds silly, but it illustrates the point that you are in control of it and how it is used.

So when you get a crank call or are in the least bit uncomfortable with the direction the call is taking, don't be afraid to simply hang up. You have no obligation to be polite or to speak to anyone against your will. If you do receive a crank call, don't react emotionally, but instead calmly ask the caller's identity: they just might tell you. But regardless of whether they do or don't, hang up immediately. Use caller ID if you can, both to keep a log of such calls and to report them to the telephone company—and to the police if the caller threatened you in any way.

If you don't have caller ID, most local telephone systems offer another alternative, usually detailed in the front of the phone book. You can hang up and then pick up and listen for a dial tone. Dial *57 to actuate an automatic trace of the last call. Wait to hear the outcome of the trace and enter it into the log. If you can get a series of such traces, you can call the phone company and initiate a complaint procedure. They will react on your behalf and may even take legal action or bring police into the matter, but they won't ever release the caller's identity to you. For more information on caller ID and other services, see your phone book, and read the FBI memorandum reproduced in Appendix IV.

Keep in mind that the caller is trying to get you to react in some expected way—typically hoping to frighten you or make you angry. If you don't give them satisfaction, you give them no reason to call again. But there are other types of caller problems you should also be aware of.

Avoid callers seeking information. Anyone who asks, "Who is this? What number have I reached?" or starts trying to interview you for demographic data should probably be put off. "Who are you trying to reach? What number are you trying to reach?" These should be your responses to this type of call. Verify the credentials of callers seeking demographic information—then decide if you wish to participate. Keep in mind that a clever enemy can use such a call to gather information useful to them. Don't fall into their trap.

You also want to watch out for people who attempt to find out if you live alone or who else may live with you. If they don't know, they don't have any business asking. Teach your children, especially, not to give away information which betrays family security. It may be safest to tell them not to answer the phone at all, and rely upon an answering machine or answering service to find who called.

Another kind of call to watch for is the "silence and hang up" call. The phone rings. You answer. You can hear someone is their, but they do not respond, even if you repeat your hello. At some point, usually sooner than later, they simply hang up. Very rude, yes, and seldom is it a meaningless event. While it is possible that someone simply dialed a wrong number and was unable to deal with the discovery in a polite manner, it's not likely.

There are several less-than-sinister reasons for this kind of call. One might be that the caller was expecting one person but got another and, for whatever reasons, was afraid to let the second per-

son know that the caller was trying to speak to the first. A secret lover involved in a triangle, for instance, or the young suitor of a daughter afraid of her parents' disapproval. Other reasons might be more sinister. One is that the caller may be attempting to find out if you are home. This might be because they plan some bit of nastiness that requires you to be away—such as a burglary. Much worse, it may be because the nastiness requires you to be there.

Another sinister purpose is pure harassment. At the height of my problems, everyone in our family (three households' worth of folks) regularly received such phone calls. You could almost set your watch by them. The telephone company said all of them were untraceable, which should tell you something about the sophistication of the caller. It was simply part of a psychological warfare effort. Consider getting an unlisted phone number or changing your number if you need to get a handle on these issues and don't seem to be having much success any other way.

The TSC/TSCM Survey

If you do worry about your telephones being bugged or other types of electronic security, you should understand the complexity of the subject before attempting to directly address the problem yourself. A review of Appendix IV would be in order if you have not already done so. Any such review might help you to consider seeking professional help. If you elect to contract a professional such as Mr. Atkinson or Tim Johnson, whose contributions follow shortly, to perform a TSC/TSCM survey, you will find the following information helpful. To begin with, you should NEVER casually contact TSC professionals. You SHOULD go well outside your local area before attempting to do so. There is a significant danger that local professionals may have affiliation with your enemy. Another reason is that you need to be well away from surveillance in order to make unobserved contact with the TSC expert. Any suspicion that you are seeking professional help can result in the target bugs being temporarily deactivated. If you contract a professional survey and the bugs are off, you'll gain nothing and waste thousands of dollars.

Mr. Atkinson suggests there are perhaps only six or eight legitimate and competent TSC firms in the U.S., and he warns to watch out for what he describes as "two week wonders," or students of TSC schools whose knowledge may stem from only one or two

weeks of classroom training. As anyone may apply and be accepted to some of these schools, the student may have little or no technical, legal, law-enforcement, investigative, or intelligence background. A good professional will have an extensive background in these areas.

The following questionnaire should illustrate how exhaustive a professional pre-screening can be. It is reproduced (in edited form) from Tim Johnson's *Technical Surveillance Countermeasures Services Manual*.

1. Site/contact basics: Your Title/Function; address; telephone no.; Manager; Assistant Manager; Human Resources Superintendent; Security Control Superintendent; Number of employees; area covered (acres); operating hours; products manufactured/project descriptions.
2. Review last finance department audit of this site for any exceptions relating to security. Were there irregularities, such as embezzlement or faked invoice payments, and what was the response?
3. Since the last survey, has the site terminated anyone for theft, fraud, or drug-related activities?
4. Have any investigations been conducted on the site since the last survey?
5. Survey should include review of theft reports prepared by this site for an appropriate period of time. Where appropriate, has corrective action been taken? Do theft reports reflect patterns, trends, or particular problems at this location?
6. What do you regard as the most prevalent or serious security problems?
7. Has the person responsible for day-to-day site security received any formal training?
8. What are the site's most theft-attractive assets?
9. Does your company deal in precious metals, controlled substances, or precursor chemicals?
10. Does the site have the latest revision of the Precursor Chemical List?
11. Identify off-site locations that should be included in the survey.
12. Does the site have a security committee? Who are the members, does membership rotate (and how often), and how often do they meet?
13. Is the site properly posted with respect to search and trespass?

14. What police agency has jurisdiction over the site? Does the plant have a dedicated phone line to this agency? Has management established a relationship? Have they been called on in the recent past, and if so, how did they respond? Do they normally include any of your site's perimeter in their patrols?
15. Are police emergency numbers readily available to plant security personnel?
16. Is information readily available on how to reach the proper agency for assistance with illegal narcotics, bomb threats, obscene calls, etc.?
17. Do you have a policy of reporting identifiable items of stolen property to the local police?
18. Does your law enforcement agency have a crime prevention unit qualified to speak on such topics as drug abuse, personal and residential security, and highway safety?
19. Is your site's perimeter adequately lighted?
20. Is the site's lighting checked on a regular basis to be certain it is functioning properly? How frequently and by whom?
21. Is the lighting compatible with Closed-Circuit Television?
22. Is the power supply adequately protected?
23. Is the lighting properly maintained and cleaned?
24. Are sensitive areas (parking lots, computer areas, stores, tool rooms, shipping/receiving areas) adequately lighted?
25. Do you have your own security, or do you contract security from an outside firm? If contract, name the agency and telephone number. If proprietary, how are personnel selected? Security Officer pay rate? Is there a high rate of employee turnover?
26. Are posts rotated and how often?
27. How many officers per shift?
28. What type of training and supervision do officers receive? Where a solitary security officer is on duty after normal business hours, is there a procedure in place requiring that individual to check in periodically? Do security officers possess any type of weapons, such as firearms, mace, nightsticks, etc.? Is there a written policy governing the use of such weapons? Has the security team received training?
29. Are security facilities adequate?
30. Is a sign-in sheet maintained at the gate house?
31. Is an incident log maintained?
32. Is the log reviewed? How often and by whom?

33. Are security personnel used for non-security-related duties?
34. Does the site use photo ID cards?
35. Does facility have on-site parking? Are vehicles registered? Can an individual reach a vehicle without passing a guard?
36. Does the security force have a patrol vehicle?
37. Does the site have a receptionist? Are visitors required to sign in at the front desk? Are they provided with an ID or visitor's badge? Are visitors escorted while on site?
38. Is the site completely fenced? Describe the type of fencing.
39. Is it secure, especially on uneven terrain? Are there rivers, ponds, trees, or buildings on the perimeter that can be used for unauthorized entry?
40. Is a clear zone maintained around the entire perimeter, on each side of the fence?
41. If building walls form part of the perimeter, are all doors and windows secure? Can entry be achieved via the roof? Can hinge pins be removed from doors? Are all entry/exit points manned while open? Is fence line patrolled? How often? By vehicle or on foot?
42. With whom does administrative control rest?
43. Do you keep track of who has keys?
44. Is a master key system in use? How many grandmasters/master keys have been issued?
45. Is a cross-control system (name versus key number) in use? What type of numbering system is in use? Are keys, including blanks, inventoried on a regular basis?
46. Are keys stamped "Do Not Duplicate?"
47. What level of management authorization is required for issuance of keys?
48. Are plant keys, particularly masters, permitted to be taken home? Are keys signed in/out in a log?
49. Are locks changed on a regular basis?
50. How long has the present lock/key system been in use?
51. Have keys been reported lost or stolen?
52. Is a record of the locations of safes and their combinations maintained?
53. How frequently are combinations changed?
54. Is an electronic alarm system in use?
55. Is a card-access system in use?
56. Do alarms terminate on the site or at an outside central station?

57. Who responds to alarms? Has service/response been satisfactory?
58. Does the site have a radio network? Separate frequency for security? Battery backup?
59. Are portable radios, chargers, and cellular phones properly secured when not in use?
60. Does the site have a program of pedestrian inspections?
61. What is the frequency of these inspections?
62. Does this location have a vehicular inspection program? Describe procedures.
63. Does this location have a locker inspection program? Describe procedures.
64. Does the site have a policy of marking theft sensitive items such as computers, VCRs, electronic scales, and hand tools as company property? Is a list of such items maintained?
65. Are serial numbers of all items recorded?
66. In the event of theft, is this information furnished to the police?
67. Are items susceptible to theft left in the open?
68. Are trash receptacles periodically inspected?
69. Can the trash receptacles be locked at night?
70. Is the trash truck followed to the dump on a random, but fairly regular, basis?
71. Is scrap metal segregated by type? Does the site have a salvage program? Are printer sequentially numbered scrap passes used? Does security inspect scrap items versus the pass?
72. Describe the site's tool room. How are tools checked in and out, tracked, inventoried, and maintained?
73. What is the procedure during off hours? Are staff allowed to take tools home or provide their own tools?
74. Are all supply stores attended when open? What is the procedure for admittance when no attendant is present?
75. Is access to telephone switching equipment restricted?
76. Are shipping/receiving functions performed from the same dock?
77. Does that area have secure facilities (lockable cages) for valuable items?
78. Are these items checked/inventoried regularly?
79. Is anyone other than shipping/receiving personnel permitted in the area?
80. Is there a restricted waiting area for drivers?

81. Are seals used on packages?
82. Is documentation for Federal Express and UPS shipments spot checked and audited?
83. Is there a truck or railroad scale on site? Is it operable or accessible to non-personnel? How is the operation supervised?
84. Do you use printer sequentially numbered weight tickets?
85. Who performs custodial services?
86. Are they bonded?
87. Are they required to wear ID badges?
88. Which areas are serviced?
89. Are they inspected by guards as they leave? Are the janitors' vehicles inspected as they leave?
90. Do the janitors have access to restricted or sensitive areas (shipping/receiving, stores, tools, computers)?
91. Are the janitors permitted to take keys off the site with them?
92. How much cash is kept on site?
93. Where are checks held?
94. Consider the products you manufacture, the required raw materials or intermediates, the your site's location and neighborhood, and the amount of cash kept on site. How do you assess your vulnerability to robbery?
95. Is fuel stored on site? Who has access to it?
96. Is there a monitoring procedure for fuel consumption?
97. Do you keep critical information on site? How vulnerable is this information to unauthorized access and reproduction?
98. Describe site's policies regarding sensitive documents, including storage, reproduction, and distribution procedures.
99. Does the site have a sensitive-documents Committee?
100. Are sensitive-documents posters in evidence?
101. Is copying equipment locked after hours, or can anyone use it? Are fax machines located behind lockable doors?
102. Are PIP inspections made during off hours?
103. Do you have a specific method for destroying sensitive proprietary information? Is anyone at this site involved in the acquisition of competitive intelligence?
104. Are background checks conducted prior to employment?
105. Is previous employment verified?
106. Are personnel and medical records properly safeguarded?
107. Are security issues included in the new hire's orientation?

108. Is company property (credit cards, ID, keys, etc.) retrieved during exit interviews?
109. Do you have a current bomb-threat procedure?
110. Who implements it?
111. Does the procedure include a check list for the switchboard operator?
112. Is there a contingency plan for acts of violence?
113. Does the site have and up-to-date strike plan?
114. If personnel are required to work alone, are they periodically checked?
115. Identify the most critical areas of the site. Are alarms in place for these areas?
116. Have you assigned a company spokesperson, in the event of an emergency/disaster situation?
117. Has the site received a copy of Electronic Information Security (ELIS) standards? Are you working toward complete implementation?
118. Does someone monitor for evidence of computer hacking and/or improper use of data-processing facilities by employees? Has anyone been terminated for improper use of DP function/systems since the last survey?
119. Are records kept to ensure that a person cannot leave a site with company property?
120. Are site employees aware of rules on reproducing copyrighted or licensed software? Have you reviewed all computers to ensure that all software is licensed? Are all personnel aware of the dangers of introducing outside (possibly contaminated) software into company systems?
121. Is access to server/mainframe rooms restricted? Locked when not in use? Visited by patrolling guards?
122. Are terminated employees immediately cut off from access to electronic information? Are their passwords invalidated?
123. Is there a tape library, separate from server room?
124. Are laptop computers locked in cabinets/closets when not in use? Are they branded/marked?
125. Are users aware of good electronic-information security practices and the ramifications of not following these practices? Do users have someone to go to for help?
126. Are passwords checked for conformity with ELIS Standards regarding structure, minimum length, and expiration? Do users write down their passwords or share them with others?

127. Have all critical software applications been included in a disaster recovery plan, and has that plan been tested? Do computer owners back up their data on a regular basis?
128. Do users leave applications open while they are out of the office? Is confidential information left on screen?
129. Do travelers leave portable computers unattended in their hotel rooms? Is confidential information displayed on the screen of portable computers in public locations?
130. Do application programmers (those who maintain/change an application's source code) have the system access to install revised code in a production environment?
131. Do employees with cellular phones discuss confidential information on them? Do employees access their voice mail via cellular phone?
132. Are requests for Email accounts on company computers for non-employees evaluated for suitability of MCI mail instead? Are accounts for non-employees on company computers documented using ELIS Form 0002?
133. Are computer rooms, telecommunications rooms, wiring closets, PBX rooms, etc., locked at all times? Are there computer rooms with sealed air systems, false floors, special computer cable runs?
134. Are all electronic documents destroyed past a given date?
135. What overall security improvements do you feel could be made at this location?
136. Can videotapes or photographs of interior/exterior be made available? Can blueprints be made available to us, detailing layout, electrical, HVAC, telephone, or computer network and plumbing locations, access points, and crawl ways? [Ed. note: Additionally, are blueprints, or other technical layout specifications maintained in a secure manner? How is access controlled?]
137. What are the manufacturer model numbers, quantities, and locations for various telephone system components, and fax and copier machines, and who uses these systems for what purpose in each location?
138. What brand/model computer system, operating system, and software is in use at what locations, by whom, and for what purpose?
139. Are records of utility bills (especially phone/cellular/pager/beeper) and repair work available?

140. Are there other tenants in the building?
141. What actions are intended if a bug is located? Is the client willing to go to authorities or file a law suit? Will documentation or other legal proofs be required?

Do It Yourself?

If you hire a professional, be prepared to spend around $250 for an initial consultation. Actual surveys can cost anywhere between $1,000 and $20,000. Or, if you prefer, you could go against conventional wisdom and purchase sophisticated equipment to become your own TSC resource. There are two choices with some practical value, though they vary from each other in the extreme. The first is an inexpensive solution for low-grade threats, and a handy device to have around the house for a variety of other reasons, such as checking the safety of your microwave oven. This is the TriField Meter, commonly available at electronics shops. I bought mine for $150. TriField is a registered trademark of W.B. Lee. An accompanying uncopyrighted data sheet, which chiefly focuses on use of the meter for health protections, makes for interesting reading, as well. Much of the data sheet is included here primarily because these issues can be important to anyone who is being targeted by mind-control technologies that involve continuous bombardment by radio and/or microwave sources, as discussed elsewhere in this work. The TriField meter can be effective in detecting such a use, despite the sophisticated nature of such attacks.

TriField Meter Data Sheet

Although not yet proven, direct and indirect evidence suggests that AC electric and magnetic fields increase the risk of certain cancers (such as leukemia and primary brain tumors) and other physiological and psychological abnormalities (some people report a difficulty in concentrating when exposed to high levels of magnetism, and some studies suggest that fields suppress the production of the sleep-inducing chemical melatonin). Although how this happens is not fully understood, both magnetic and electric AC fields that surround the body can produce AC electric current inside the body. The best available theory is that this current interferes with the normal transport of ions across cell membranes. At

a continuous exposure of about one billionth of an amp of AC current per square centimeter (give or take a factor of three), biological effects begin to be observed. Very preliminary results show that at five times that level, for example, an increase in protein production in cancer cells is seen; but when the field is increased 1,000 times further, the increase in protein production is only three times greater (not 1,000 times greater). These changes are seen for AC current at several different frequencies, including 50 Hz.

If the cell-membrane-interference theory is correct, the body should be sensitive to current at any frequency up to about 1,000 Hz; above that, sensitivity will decrease (the exact frequency is not known and experimental measurement of it has not been attempted). The currents induced by artificial fields may also affect the nervous system directly, and the evidence of this is somewhat stronger than that of the cancer effect. Exposure to a fairly strong magnetic field of 300 milliGauss (at 60 Hz) will consistently slow down subject's heart rates by about three beats per minute for three or four minutes after the field is turned on, even thought subjects cannot directly sense the field. This field strength is the strongest typically encountered in the home, but weaker fields may produce more subtle effects that take longer to manifest themselves.

Based on the above evidence and some epidemiological studies, it would be prudent to avoid continuous exposure to any electromagnetic pollution that produces AC current inside the body higher than one billionth amp per square centimeter, at frequencies of 1,000 Hz or below. (No absolute hazard threshold has been established yet, but the lower limit for biological effects is probably give or take a factor of three from that level. Preliminary results also suggest that it's better to spend a short time well above this threshold than a long time just above it.) At frequencies above 1,000 Hz, the body is likely also to be sensitive, but not as sensitive as it is to lower-frequency current.

An external magnetic field of 3 milliGauss or an electric field of 2.5 kilovolts/meter at 60 Hz will produce approximately one billionth amp per square centimeter. The current produce inside the body is proportional to field strength times frequency, so at 120 Hz (twice the frequency), only half as much field (i.e., 1.5 milliGauss and 1.25 kilovolts/meter, respectively) is required to produce the same current inside the body. Interestingly, a fairly strong magnetic field (500 milliGauss) and electric field (about 2 kilovolts/meter) exist in nature, but these fields are static, and

thus have a frequency of zero—they produce no current inside the body.

Any measurements of electromagnetic pollution should probably be frequency weighted, meaning that they read the product of magnetic field straight times frequency and/or electric field strength times frequency, if the measurements are to gauge whether the current inside the body exceeds a threshold level. This frequency-weighting should extend up to about 1,000 Hz and then sensitivity should decrease at higher frequencies. Previous measurements that looked for a link between cancer and field strength have used several types of metering; some frequency weighted, some not, and some measuring only 60 Hz fields (or 50 Hz outside of North America). Different types of meters read differently, thus making more difficult to establish meaningful interpretations.

Magnetic and electric fields are vector quantities. This means they are specified as having a magnitude (or field strength, measured in milliGauss or kiloVolts/meter respectively) as well as a direction (an arrow showing which way they are pointing). The effect on the body is more or less independent of the direction of the field; only the magnitude is important. Many of the measurements of possible cancer-field links were of the field strength in one direction only. The sensor in these measurements had to be pointed in the same direction as the field was pointing; otherwise, the reading would be less than the true magnitude of the field strength. (If the sensor were erroneously pointed perpendicular to the local field direction, the reading would be zero, no matter how strong the field actually was.) To avoid this inaccuracy, all studies should be done with meters that read the true magnitude of the field, so a researcher should walk through a room with a meter and get an accurate, immediate reading of the field magnitude at every point along the path, regardless of which way the meter is oriented.

One more matter that complicates the interpretation of the strength of fields has to do with how magnetic fields induce current in the body. The current per area induced is proportional to field strength times frequency times the length of the body. For this reason, children exposed to magnetic fields experience less current per area than do adults, and lab rats experience about 1/10th as much. The multiplication by body length does not apply to electric fields, however (so a rat would experience the same current as a human, when exposed to an electric field).

The TriField meter combines all the features needed for fast, accurate measurements of electromagnetic pollution. It independently measures electric field and magnetic field and is properly scaled for both, to indicate the full magnitude of currents produced by each type of field inside the human body. As a result, it sees much more than any other electromagnetic pollution meter. Depending on where the knob is set, it detects either frequency-weighted magnetic fields (two separate scales) or frequency-weighted electric fields in the ELF and VLF range (it has significant sensitivity at 100 kHz, well past the 17 kHz horizontal scan of video displays). It also has a setting which lets you gauge radio-wave power all the way up to 3 GHz, CB and cellular phone equipment, and many radars.

This meter is the only one which combines magnetic, electric, and radio/microwave detectors in one package, so the entire non-ionizing (that is, not including nuclear radiation) electromagnetic pollution spectrum is covered. In addition, the magnetic setting and the electric setting measure true magnitude, a feature found elsewhere only in more expensive meters. If you hold the meter in the center of a room and tip it to various angles, the magnetic reading will stay approximately the same (± 15 percent, typical), regardless of which way you tip or rotate it. The electric reading is similar, although the presence of the human body alters the actual electric field, so readings will vary more. The radio/microwave setting reads full power of radio waves radiated into the front of the meter. Radio and microwaves are composed of a particular combination of electric fields and magnetic fields that is self-sustaining. For frequencies below about 100 MHz, the principle effect on the human body is from the magnetic field only. This is because the electric-field component of radio waves produces much weaker currents in the body than does the magnetic field, unless the wavelength of the waves is smaller than the height of the body. Low-frequency electric fields by themselves can be strong enough to create significant current, but only if they are from sources other than true radio waves.

The radio/microwave resolution in the low range is 0.01 mW/cm2, which is the Russian standard for maximum safe microwave exposure to avoid changes in brain activity , and is the most conservative standard of any country. In contrast, the U.S. legal maximum is 1,000 times higher, at 10mW/cm2, but only brief exposure is allowed at this level. As mentioned earlier, a true radio

wave is a particular combination of electric and magnetic fields.

In most homes or offices, some areas are hot spots with readings in the HIGH range on one or more settings of the meter. Most often, this is caused by magnetic fields, which come largely from unrepaired internal wiring. (Contrary to popular belief, power transmission lines and transformers do not generally contribute as much magnetic field as does internal wiring.) Other magnetic sources include video displays, motorized clocks and other equipment, electric blankets and heaters, fluorescent lights and light dimmers, and the transformers that are inside consumer devices. Many of the effects are from frequencies that are harmonics, or multiples of 60 Hz (120 Hz, 180 Hz, etc.) and 17 kHz of video displays (computer monitors). Cars (especially toward the front of the floorboard in electronic-ignition cars) and motorcycles have fairly strong fields that are at frequencies higher than 60 Hz. Magnetic fields are difficult to shield against, but sheet steel is somewhat effective.

Occasionally, certain areas read HIGH in the radio/microwave detection mode. These include door seals around microwave ovens, and cellular phones (but not regular radio phones, which operate on very little power). Radio/microwaves can be shielded in the same way as electric fields, although the lower-frequency radio waves are not shielded as easily as microwaves are. (Metal screens will shield both). In the U.S., radars and FM transmitters can legally expose residents to moderately high power levels (as high as 10 mW/cm2), but such exposure is not common.

By seeing hot spots in your home and office, you can move furniture, cribs, or beds to reduce exposure. You can also take corrective action to avoid long-term exposure to appliances that emit high electromagnetic pollution levels. If you have unusual sensitivity to a particular type of field, you can identify where problems exist. Those who use pacemakers should avoid even brief exposure to high radio/microwave power levels. There is also evidence that suggests that even brief exposure to very high AC electric or magnetic fields may cause nervousness or seizures in some people.

As a bug detector, the TriField meter can find devices which operate as high as 3 GHz (same as more sophisticated bug detectors), provided their emission strength and proximity is adequate (the better detectors won't be so limited). The TriField Meter is an extremely simple but sensitive hand-held device which provides a way to detect and measure magnetic, electronic, radio, and

microwave sources. As an electronic bug detector, it is passable for only the crudest devices. It is certainly no match for the type of devices likely to be applied by federal agencies, particularly those which operate on multiple frequencies or extremely low output transmitters.

To use the TriField meter for this purpose will require that you set it to the Radio sensing position and run it directly in front of (as close as possible within an inch) every square inch of any potential hiding place for a transmitter. The meter cannot detect microphones, so any device which runs a wire to a separate transmitter further away cannot be detected—only the transmitter can. Because there are spike (nail-like) listening devices which can be driven into walls, ceilings, or even floors, and since they are often no larger at the visible end than the tip of a ballpoint pen, you should carefully and routinely scan every inch of surface area within the suspect room. This includes furnishings and all other objects. In particular, scan all sides of three-dimensional objects, with careful attention to concealed or out-of-sight portions, known hollow areas, lips, overhangs, etc. Also pay special attention to electronic devices, as bugs need power, and ready access to power within the device makes them an attractive hiding spot. Don't forget your telephones.

Such a test will take hours of tedious and seemingly nonproductive effort. Finding a bumper beeper on a car will be much harder—you will have to put it on a lift and work with difficult lighting and undercarriage obstructions. The things might also emit an intermittent signal too brief for the detector to see. Leave the ignition key in the on or auxiliary position to insure power flows from the battery in case the device you are searching for draws power from the car. Just because a search with a TriField fails to indicate a radio source, it doesn't mean you are not bugged—it only means you didn't find one. A sophisticated or well-hidden bug might be easily missed. But a find is worth its weight in gold, and makes the effort well worth your while. A bug in hand is proof positive of a problem, and can be used as leverage for obtaining help from those who would otherwise consider you truly paranoid. It can also provide clues as to who your opponents are, and where they are operating from. A TSCM professional should be able to tell you more.

DO NOT REMOVE the device until experts have had a chance to examine it. Don't forget, it can also be a good way to impart dis-

information to your opponents. All of this, of course, requires that your search for the device be done discreetly. You won't get very far if you conduct the search while others are present and they make a comment about it.

Granite Island Group will sell the more costly OSCOR (Omni-Spectral Correlator), made by Research Electronics, to allow you to go after the more pesky little bugs yourself—whenever or wherever you like. You might even be able to market such services to others to help defray the cost, but you had better check with your state government and local law agencies for licensing requirements or other prohibitions. And if you do, bear in mind that you'd be just another one of those two-week wonders with inadequate equipment for full-scale TSCM services, which the pros frown upon as ripoff artists. Still, for about a $15,000 hardware investment, plus another $6,000 to 10,000 for training, the OSC-5000 provides a compact "carry-on" piece of equipment for Automated Spectrum Monitoring and In-Place RF Monitoring. The OSCOR combines all the functions of a switched and amplified antenna array, peak-detection circuitry, wideband search receiver, demodulator, audio correlator, computer controller, LCD display panel, and hardcopy printer—in one customized, briefcase-sized package.

The OSCOR Advantage

1. Portable and programmable operation that continuously scans all bands and silently detects eavesdropping equipment.
2. Complete package of sweep equipment, including a set of sweep antennas with automatic switching. All equipment folds into a single, highly durable briefcase, with room for future modules, probes, or cables within the upper storage compartment.
3. High-sensitivity digital receiver scans audio from 50 Hz to 5 kHz, RF from 10 kHz to 3 GHz, and infrared from 850 to 1070 nm.
4. Audio-analyze mode demodulates a received signal to audio and provides audio signal lock to support correlation.
5. Acoustic correlator uses passive sound-pattern matching to automatically detect a listening device.

6. Strip chart plotter provides plotting of threat lists and all available signal analysis screens; provides a hard copy of important data.
7. Signal database provides storage and recall of all detected signals.
8. Operates at 115 and 230 VAC, comes with internal, rechargeable 12 VDC battery, accepts external 12 to 18 VDC input.

Night Vision

I have had the pleasure of sampling several inexpensive Soviet-made night scopes which have since become available through gun shops, sporting goods stores, and specialty outlets here in the United States. This proved to be a learning experience that not only provided basic training on the technology but also revealed that my opponents were using night-vision technology to watch me!

These devices amplify the visible or infrared (IR) light spectrums electronically, using technology derived from television cameras. There are two types, passive, and active. A passive device simply amplifies existing light. These do not work as well in total or near-total darkness. An active device, however, emits its own infrared light source for reflection and detection by the viewer, and it works in absolute darkness. An active unit will usually have a switch to power down the active source (to avoid detection by night scope–equipped enemies).

Other variations include monocular and binocular design, tripod mount and camera mount to allow for use of infrared film or low-light videocameras, pistol grips to steady aim, built-in or slip-on neutral density filters to combat bright light sources in the viewing area (to avoid damaging your eyes or the units). Some even have zoom functions.

Territory Defense

There are a number of introductory things to discuss here. To begin with, a well-maintained home or business that demonstrates occupancy and continued care is an excellent deterrent to burglary. Any security systems you may put in place have no value unless used religiously. In addition, good neighbors know each other, watch each other's back, know each other's habits and acquaintances, and call the police whenever in doubt. If security is not something you think about regularly, then you don't have any. If you think about it a lot (and follow through), then you are much more secure. You should assess your security level frequently, playing the role of would-be burglar. How would you get past your own security, knowing how it's set up? If you can figure out how to get past your security, they most certainly can. Get a professional opinion. Most local police will be happy to provide this service, as would most alarm companies (they have a good motive to find your weaknesses!).

There is a simple test you can take to determine your vulnerability based on well-understood statistics and probabilities. This is available on the Internet by visiting www.nashville.net/~police/risk. There are actually three different tests: 1) Rate Your Risk of Being Murdered, 2) Rate Your Risk of Burglary, and 3) Rate Your Risk of Serious Assault. You can take the tests in minutes, get an answer, and then try changing answers for things over which you have control. Retake the test to find out how important such a move may be. For me, forming a local Neighborhood Watch program would net a 45 percent reduction in likelihood of burglary, according the burglary test.

Early Warning Systems

Think about your home or office in terms of defensible zones. Which currently offer sufficient protection, and which are exposed? Are there areas that offer opportunities for additional layers of defense? Your thinking should not be limited to your property line. Find ways turn your immediate neighborhood into part of your defense. Get to know your neighbors. If you are located on high ground or have other visibility advantages, a video security camera might extend your viewing range significantly beyond your property line.

A good fence and locking gate or a network of fences, shrubs, and other barriers can serve as an excellent deterrent. Consider

installing motion-activated lights on your property. Motion detectors can also be used to trigger cameras and alarms. Other early warning tools which can work as well as motion detectors are trip wires or noisemakers placed so as to catch intruders off guard.

Next, think about the exterior of the building. Don't overlook roof, basement, vents, and other points of entry. Consult a locksmith or security expert for specific advice. I like the Primus pick-proof lock system, which is only available from select locksmiths. It is a relatively conventional looking key-and-lock set, but it uses a second set of perpendicular tumblers. Not only is the Primus virtually impossible to pick, but it comes with other benefits, as well. First, there are few dealers which sell the lock, and each dealer is issued a unique set of key blanks and a special key-making machine required to mate with them. Only the dealer from which you purchase a Primus lock can make a key for it, and they must keep their key-making machine in a vault as part of their dealer agreement. The key blanks and documentation on owners are also kept in the vault. Finally, no additional keys will be made, even with the original in hand, except under certain circumstances. That is, that each Primus purchaser is issued an ID card which matches a client slip kept with the key blanks. Only by presenting the card can one order extra keys.

Part of your plan should include an alarm system which protects all entry ways and outer rooms. But the layered defensive approach can be continued even within the home. Individual rooms or groups of room, hallways, etc., can be treated as zones and protected with alarm systems which independently protect these areas. A good system might let you know the progress of anyone who gains entry. Even without an expensive alarm system, you can use several individual motion detectors to do the same job, or even set noisemaker traps.

Nobody Home

Your concerns may be entirely different when you leave your house than when at home. Personal safety is always more important than the safety of objects or information, unless you are willing to die for what you are protecting. Depending on your opponents and your strategy, you might even want them to enter and obtain goodies you have deliberately left for them. There are times when it is desirable to allow or impossible to deter such entry.

By the way, unless you make illicit entry so difficult that the only way in is by breaking and entering, you normally can trust your opponents not to fool with your valuables. If they gain entry to gather information, for instance, they wouldn't dream of actually stealing something valuable left out in plain view. You could leave stacks of hundred dollar bills, and they wouldn't touch it. There is the chance, however, that they would steal something to make a forced entry appear to be part of a simple burglary.

If you do deliberately leave something for them to find, don't make it too easy. If it isn't hidden, they'll be suspicious. Make them dig for it, and in the process, leave some trip indicators so you know the bait was taken. This can be most gratifying. If you set your indicators properly, they can't be seen prior to tripping, and even if your enemies realize what has happened, they won't be able to do anything about it. If you set enough of them, you can determine their entry point and progress through the house. You might even know when they did it, and if you have a good neighborhood watch, you might have vehicle identification (they will likely have parked well away, unless they were concerned about a fast getaway).

When leaving and especially when expecting company while away, ask your neighbors to keep an eye out. They could call the police or just observe. You needn't do this in a way that causes undue alarm or fear of increased crime in the neighborhood, and certainly, you need not involve them greatly with your problems.

Snug As A Bug

When home at night, there are a number of things that you can do if you expect trouble. Normally, if your opponent is aware of your presence at home, they will not attempt entry unless foul play is intended—or they are extremely competent in surreptitious methods. If your early warning system works properly, you will not only be alerted to a problem but will likely know where the point of entry is. Better still, you may be able to follow their progress through the building by the noisemakers you have placed. Stairwells are particularly defensible if you hold the high ground. You can lay low behind the lip of the topmost step, exposing only your forehead.

Keep a few items handy if you expect company. With a bright flashlight, you can both spot and blind your opponent (and draw their fire away). Use a passive night scope, too, for your opponent

will likely be using active, and you will see if they are approaching by the infrared light they throw off. And a camera of some type, especially one with a blinding, brilliant flash, could make for an interesting weapon!

Your best defense, both during a crisis and in terms of legal aftermath, may be to call for help. Even if you don't believe you can trust law enforcement, that step should still be a part of your game plan. Don't rely on the house phone, for the lines might be cut. Have a cellular phone ready to go, one with illuminated buttons. Preprogram the number for your local police's emergency line, and you're all set. You might also preprogram your neighbors' numbers so that you can alert them.

You might still wish to make entry by any means other than force impossible. For instance, I have deadbolts and other locks safety-wired so that they could not be operated even with a key. This forces noisy entry methods and buys you time. It also means you are prisoner in your own home and may have some difficulty getting out in a fire or other emergency. In this event, keep wire cutters or other quick-release methods handy for whatever means of blockage you have created.

Under Siege

If you expect to come under overt, armed attack by a superior force, there is likely no defensive tactic that will buy your freedom. You opponent will overpower you, eventually. So rather than focusing on resistance, your best bet in this circumstance is to focus on delaying your enemy, maintaining your personal safety, and enabling your escape. Any action you can take to survive a barrage of gunfire or tear gas is in order. Anything you can do to prolong the affair will help to assure news coverage, which is favorable.

There are other suggestions that you may not have yet considered. Walls can be filled with sand by drilling large holes between studs near the ceiling. It is tedious work, but it should stop almost anything short of a tank round (it's also a very good, low-budget soundproofing technique). Windows and doors can be buttressed with movable walls that can block these entrances entirely. A couple of two-by-fours placed in brackets screwed into the door frame will brace against battering rams.

You should likely have an inner room of solid cement or filled cinder block construction which is ventilated and fully equipped for

long-term survival. You will need outside communications, but other than that, soundproofing would be good, as your enemy could try audio-based psychological warfare (i.e., blaring music 24 hours a day) on you. Anything along these lines has to be done in secret, so it is the rare situation that supports these kinds of measures.

If you recall the incident at Waco, the government ensured there was no escape. The only safe place was an underground "escape tunnel" to a bus which had been buried for just such an attack. This is where Branch Davidians elected to hide the children. The bus had an air vent to the outside. The BATF carefully moved their armored vehicle over this hiding spot, and through the bottom of the vehicle, they dug a hole down to the top of the bus, and drilled through. They then proceeded to fill the bus with CS-4 tear gas in deadly quantities. CS-4, being flammable, ignited (possibly by government forces). All the children were killed. See the motion picture *Waco—the Rules of Engagement* for all the terrible details.

The point is, there was no real escape. Any real escape will likely need to be via an underground passage. The Davidians did not consider infrared capabilities, which was used to detect their relatively shallow underground tunnel and buried bus. They also underestimated the ruthlessness of their government. You should not. Should you elect to defend against such an enemy, any tunnels must be very, very deep to avoid detection. Exit points must well concealed and well away from your main building. There should be no air vents, but fresh air can be provided by forced ventilation, which should be at the same temperature as the ground at that depth. The proper depth, according to FLIR detection system descriptions I've been given would be 36". From the lessons we've learned at Waco, we know this is not enough, likely a deliberate deception by the government. I'd go down a minimum of twelve feet—and this means a very well-dug, reinforced tunnel, so as to avoid the risk of collapse and water-seepage problems.

Cause for Alarm

Every situation is different when it comes to selecting an alarm system. Experts can suggest whole systems based on what you need and how much you can afford. Having worked in that industry, I can offer some basic advice. Alarms can be anything from simple noisemakers to devices which call police, alert alarm-company monitoring facilities, and allow listen-in capabilities (not a good idea if you

are worried about eavesdroppers, as such systems could be subverted and used against you). There are paneled alarm systems which are the owner's responsibility, and there are alarm-service companies that automate the entire affair. My advice is again to go for a layered approach and not put all your eggs in one basket.

A good perimeter penetration alarm system is good, but I like to additionally put touch-capacitive alarms on key entry points—such that simply placing a hand, even a gloved hand, on a door knob will trip the alarm. Where that will not work, consider motion detectors to do the same. Detect them before they gain entry, if you can. Also consider bolstering any main system with individual room motion-detector systems. Again, this redundant system works in your favor by letting you track your enemy though the building and acts as a backup should the primary system be compromised. Combining all of this with external motion detectors and possibly cameras and automatic lights provides for a very comprehensive program. (Keep in mind that costs can quickly add up.)

Understand that your main system will need to be one of two primary types. Wired systems are very good but expensive because they require installation of wiring from the alarm panel to each window, doorway, and other sensor location in the system, in addition to the alarm mechanisms such as lights, bells, sirens, and so forth. Wireless systems are cheaper and quicker to install but use RF (radio technology) to transmit information to the control panel, sometimes by actual broadcast radio waves, sometimes by embedding the RF information into AC wiring circuits already in place throughout the house. The BSR X-10 series is such an example. These systems suffer several drawbacks, the worst being that they can be subverted to become listening devices by a knowledgeable enemy.

Another feature of alarm systems that should not be overlooked is panic buttons. You should likely have more than one, ideally a pocket or portable unit or two for family members. Have a couple hidden in logical points of detention. A quick press of a button triggers the alarm (usually a silent one). In my home, one was placed behind a picture. Leaning into it would set it off, which is probably something I could safely do if I was held at gunpoint.

Finally, with respect to alarm service providers, many of these have affiliations with, or are permeated by, federal spooks. If your problem is federal, I advise against hiring an alarm company unless you are extremely confident in their background. Frankly, the

more well known the company, the more skeptical I am. The less well known the company, the less reliable. Where does that leave you? Probably deciding to maintain your own alarm system. If you do, keep in mind that one option is to wire the alarm system into your computer, making it useful as a "peek" resource to monitor how things are going at any given moment. You may need some professional advice on the needed hardware and software, but the BSR system is very simple to interface and can be adapted to or integrated with more sophisticated systems.

Vehicular Security

I leave my car completely unlocked and, in summer, the windows down. This advice will not work for everyone, of course, but for someone like me, with a $1,000 car and a removable radio, it works just fine. I've detected no fewer than a dozen entries, three of which I knew to have involved electronic tampering. A locked car invites forced entry, which often does more damage than the value of the item(s) stolen. This same car, when locked, had been violated twice to get at the radio. The total damage to the car was over $2,000. The street value of the radios was less than $100.

I note how things are positioned in my car so that I can detect any rummaging about—something which in itself does not necessarily alarm me, since an unlocked or open car invites entry. But any indicators out of place suggest reason for more careful study. Is the clock still accurate? Any errors indicate the battery has been disconnected for a time, suggesting a bomb or a device which must draw power at all times, such as a radio bug or electronic tracker. Has the hood been opened? Human-hair indicators work pretty well. I also like to stick a pebble into the crack between the hood and fender—which falls out when the hood is opened.

Look under the tires for devices designed to cause a flat as you drive off. If you feel it necessary, use a mirror to examine the undercarriage for bombs. If you do detect a bomb, photograph it quietly before calling in experts. Later, when they claim it was just a firecracker, you'll have evidence to the contrary. I also like my friends and associates to be aware my car is unlocked, and I park in a well lit area that is under surveillance.

Psychological Issues

This work would not be complete if it did not address issues related to your state of mind under the pressures of surveillance or attack. The very title of this work suggests the obvious: Paranoia is, unfortunately, a necessary part of any such problem, you may be experiencing. The medical term has been misunderstood to the point that it has taken on extremely negative connotations.

Paranoia is a description of a certain kind of psychosis wherein someone suffers from delusions of persecution. But this is inappropriate for people who face such a problem in reality. Most people not experiencing or witnessing firsthand the events claimed as the cause of "paranoia" tend to assume these events to be imagined.

Specifically, paranoia is marked by heightened awareness, increased caution, and machinations over uncertainties and suspicions about the nature of events and intentions of people encountered in day-to-day experiences. A paranoid individual literally looks over his shoulder, continually wanting to know who is doing what and what potential danger or dark purpose may be associated with it. Often, innocent activities take on a sinister potential when filtered through an active imagination. The problem is that, in terms of behavior, there is no visible difference between a delusional paranoid and a person experiencing a real, life-threatening situation.

Unfortunately, using the term "paranoiac" for those with real problems is all too easy a position to embrace. To the individual being followed, investigated, or pursued, paranoid behavior is not an illness but merely an appropriate behavioral response to real experiences. But, as the behavior is observable and the experience driving it is typically not visible, there is a kind of flip-flop of truth and logic. While true paranoia is not common nor natural in the mentally healthy, a mentally healthy individual under the uncommon circumstance of a true problem will naturally exhibit the same traits of paranoia.

Enemy Strategies

Your enemy may well be aware of the ease with which the paranoid label can be attributed and the disadvantage such a label represents. If you are facing the intelligence community, especially,

you can expect to be labeled and your credibility could attacked.

Another tactic is to deliberately do things to cause you alarm sufficient to cause you to talk about it to others or go to the authorities even if you have no proof of the event. When I approaching law-enforcement friends and former coworkers, they immediately did the knee-jerk thing and asked if I had considered seeing a psychiatrist. Often, the natural urge to see paranoia at work can even override and neutralize the value of what little evidence you might actually have documenting your claims—as this is eagerly attributed to more innocent meanings or circumstances. Unless you have a smoking gun, a viable confession, a set of bulletholes, or a body, it's a hard nut to crack. Even then, some accusations may be thrown your way. In my case, the police actually assumed I staged events, even going so far as to ignore witnesses to the contrary because of the "mental problem" prestaging done by the first officer.

Worse, a sophisticated opponent will actually create a psychological profile on you. The CIA, for instance (who are by no means alone in this), will actually gather data on your behavioral responses to events (many planned and staged just to observe your response) and present the results, along with background data, to CIA medical experts. The Agency operates a computerized modeling system which can be programmed to project your response to a given scenario based on the psych profile. This profile is quite detailed and often accurate, and it includes a very complete section on sexual preferences and practices. These methods are used to find your areas of vulnerability and determine their approach. Indeed, there is evidence to suggest that this very technique has been used to bring members of Congress and other power figures deemed important to Agency goals "into line." It is a little-known fact that the Watergate scandal itself revolved around and involved a CIA program to capture audio/video of the sexual escapades of important and powerful people in Washington, D.C.—useful both in preparing psych profiles and in providing blackmail material. That's real influence peddling in action!

Public Perception vs. Reality

The public at large, your friends, and your associates represent a different problem. As far as any third parties or strangers are concerned, it seems to make little difference if you appear "loony" or not. The danger can be that an enemy is in a position to make that

person's experience of you available at a later date—in a courtroom, for instance, where discrediting you may be of significant value.

Friends and associates will have already known you for some time and will become aware of your change in behavior. If you try to conceal your problem, they will worry and gossip. If you tell them of your problem, they will worry and gossip. Either way, some will believe you, some will not, and some will reserve judgment. To the extent that you can determine who thinks what, you will be able to ask for help and emotional support from the faithful.

You may have to put up with very difficult situations with the others. You are likely under tremendous levels of stress, and the additional stress of exposing people to your problems (directly or indirectly) can become a significant factor. You may end up in arguments which sever or damage relationships, or you may simply end up needing to distance yourself from them. Or, you may end up having to deal with do-gooders who take steps that are well intentioned but inappropriate.

Self-Perception

As far as your sanity is concerned, all that really matters is how you view yourself and how you deal with the way others may see you. Should you become overly anxious about the opinions of others, your mental state is at risk. If you become a slave to their labels, you could begin to suffer emotionally and physically. This also serves your opponent by weakening your ability to resist.

Keep an eye on yourself for increased evidence of paranoid behavior as well as outbursts of anger or negativity at the slightest provocation. The more you understand your behavior, the more you can forgive yourself for any such episodes and resist them in the future—and the more resistant to victimization you become.

I suggest that you do as I have. Externalize the whole situation, and have fun with it. I try to view all that happens around me in such circumstances as events being played out on a stage. There are actors with parts to play and a plot within which the actors have an ability to alter the story line in real time—a kind of ad-lib performance. Try to feel less that people are doing things to you or that you are experiencing these negative events but, instead, that you are witnessing a film or a play in which you are the principal player. Try not to be the victim, but the hero—and accept that the hero must suffer some losses in order for the victory to be

glorious. Try to see everything that is happening as though it were there for your entertainment—and as an opportunity for you to act out your part.

While there is a danger that, carried to the extreme, you could experience a break with reality, this mode of thought does make it easier to calmly step back and analyze a situation, become aware of your emotions, and control situations by acting against the expected response to the given stimuli. It's all about acting—and this is a tool you can use against the psychological profile, as earlier mentioned. For instance, when anger wells up, you can choose to ignore it and act as if nothing is amiss. Or you might deliberately become enraged by almost nothing, depending on the situation. All this may require that you confide in those you trust. Anything you can along these lines do to introduce errors into any psychological profile being prepared on you will undermine its value.

I found it handy to keep a note that said, simply, "acting." I would show it whenever the need arose. The purpose of the note was made clear early on, and my wife knew to play along. We both had fun with it, sometimes launching into knock-down, drag-out fights. In a way, you can consider this primal therapy; try it for fun even if you don't think someone is listening, and see what I mean.

I'd also like to mention here that, if dealing with the CIA, or others intent on bugging your bedroom, you will need to address the matter of having sex in a an "audience" environment. My wife was, at first, reluctant to have sex at all. In the end, we both learned to ignore it entirely. In fact, I sometimes deliberately acted out of character when I thought the event was being observed, just to throw inaccuracies into their profile. Keep in mind that not only does your sex life keep you healthy, but those who have to listen to it suffer a certain effect, as well. They get horny, and, possibly more potent, they can come to appreciate the love and closeness you share with your partner—endearing them to you and your family. In a way, by expressing your humanity under their noses, you are conducting a sort of psychological covert counterinsurgency warfare of your own against your enemy.

The Enemy's State of Mind

It may be wise to conduct your own psychological evaluation and projections. The more you can "get inside" your opponent's mind, the better you can anticipate his actions, take steps which dictate his

actions, and, ultimately, defeat him. Use your best judgment of human nature, and base your opinions and decisions on your own experience and intuition. The typical spook is very dedicated, highly motivated, and not easily turned aside. Many spooks are not motivated by ethical or moral concepts at all but are merely mercenary agents. The only chink in their armor might be fear of losing—either losing to you or losing face with their peers and superiors.

Sometimes you can spot an intelligence operative by his confidence and demeanor. They have a way of carrying themselves that is just a little too calm and controlled, as if every nuance was planned in advanced. Still, all such operatives are human, with their own frailties, problems, and emotions. Spooks have a conscience and compassion, they just suppress them. The more you express your humanity in a positive manner, the better your chances at striking a chord within them. It only takes one instance to grant a victory. It might even be the final victory. In addition, many intelligence types and other professionals are powder kegs, waiting to explode. They have redefined and molded their outer persona, endured or committed evil deeds, operated in a constant state of heightened awareness for so long that they often end up experiencing nervous breakdowns or worse. You may have to take advantage of this possibility.

Are You Out of Your Mind?

Those who scoff at the notion of mind control know nothing of the subject. Of course, those who claim to be victims of mind control may or may not be genuinely afflicted. Here you will learn what to look for if you suspect you have been targeted, and you will be shown how to deal with it. To quote several paragraphs from my own *Alice in Americaland*, a work which is based on the composite experiences of several mind-control victims to show what it is like to have be a mind-control survivor...

> CIA has spent decades in mind control research. They have had many successes, though they only talk openly of failures. They have delved into every imaginable alter-science, metaphysical nonsense, witchcraft and voodoo as well as traditional, Western-style medical and psychological research. They have butchered some minds with surgery and electro-shock therapy to

> the point of bursting brain cells, others with chemically induced altered states and radio-wave transmissions that literally cooked the brain matter, and still others with mental and physical torture, hypnosis and combinations of the above. Many people have been reduced to vegetables or made insane, and still others killed themselves, inadvertently or purposefully, to escape their torment. All these things were done to both American citizens and others by an intelligence machine which decided that the medical experiments of the Nazis during World War II had not been vile enough, even going so far as to import Nazi war criminals for the cause.

This has been well documented in many works, such as Alex Constantine's *Psychic Dictatorship in the USA*, and *Virtual Government* (both from Feral House books), or my upcoming book *Alice in Americaland*. Readers are urged to read up on CIA mind-control projects, such as Artichoke, MK Ultra, Often Chickwit, and many, many others, including hundreds of CIA projects and front operations at major universities. There is much about this topic on the Internet, and, though the info must be taken with a grain of salt, it does provide a good starting point for further research. These experiments supposedly ended in the 70s, following public exposure and Congressional investigation, and this exposure is the only reason we know as much today about it as we do. Yet there is much to suggest the experiments continue. You will find the CIA's fingerprints all over Jonestown, Guyana, and Waco, Texas.

But don't take my word for it. Atrocities aside, just consider the issue of technological feasibility. Former Military Affairs Specialist Chuck DeCaro appeared on a CNN Special Assignment program which aired in early 1997. For the show, CNN enlisted the help of noted physicist Dr. Elizabeth Rausher and electrical engineer Bill VanBise to build and test a mind-interference machine from data found in military documents of the former Soviet Union.

The machine, designed to emit a weak magnetic pulse at extremely low frequencies, was built from inexpensive parts from a consumer-electronics store. DeCaro was blindfolded, his ears were plugged, and he was put into a small room near a magnetic probe producing waveform patterns at about one one-thousandth of the

earth's magnetic field strength. At precisely the time changes were made to the machine's settings, DeCaro saw geometric shapes which he described as "flying by." VanBise concluded, "[Basically, you can induce] hallucinations in people, direct them to do things against their so-called better judgment. In three weeks, I could put together a weapon that would take care of a whole town."

DeCaro showed the results of the test to Dr. Robert Becker, a two-time Nobel nominee for his work in the biological effects of electromagnetism. Dr. Becker concluded, "This is a very significant experiment because it carries our understanding of how vision is actually performed a step further into the mystery.... That kind of a disturbance in the visual system could markedly influence [behavior]. [Ed. Note: Dr. Becker paused and did not finish the phrase before starting the next. The topic was behavior control by external stimulus, so I take the liberty of inserting it here for clarity.] Even as simple an aberration in the visual field as making everyone seeing double or everyone having their visual field jitter like a poorly-adjusted television screen." Of course, Dr. Becker didn't know CIA experiments had already gone well beyond this.

DeCaro concluded, "Is the United States military working in the field of electronic mind-control? Officially, the Department of Defense will not comment because the subject area is, quote, 'too sensitive.'" He then goes on to present the view of a Navy scientist with knowledge of Navy experiments and the technology for counter-terrorism and special operations. "It's possible to entrain a certain percentage of a population, apparently, with weak magnetic fields." The same study, DeCaro adds, "... also showed that RF signals could dissolve certain types of rat brain cells at a distance, causing disorientation and nausea."

Next, from the May 1995 issue of the Newsletter of the Bioelectromagnetics Special Interest Group (684 C.R. 535, Sumterville, FL 33585), we have an article entitled "Synthetic Telepathy" by Judy Wall. This work heavily quotes from government and scientific sources, starting with an Aerospace Medicine article which describes how, in 1961, biophysicist and engineering psychologist Allen Frey reported that humans can hear microwaves under the right conditions.

> Frey ... found that human subjects exposed to 1310 MHz and 2982 MHz microwaves at average power densities from 0.4 to 2 mW/cm2 (safe levels) perceived

> auditory sensations described as buzzing or knocking sounds. [These sounds were also described as clicks or chirps.] The peak power densities were on the order of 200 to 300 mW/cm2 and the pulse repetition frequencies varied from 200 to 400 Hz.... Frey referred to this auditory phenomenon as the RF (radio frequency) sound. The sensation occurred instantaneously at average incident power densities well below that necessary for known biological damage and appeared to originate from within or near the back of the head.

The article then cites "Microwave-Induced Acoustic Effects in Mammalian Auditory Systems and Physical Materials," from the New York Academy of Scientists in 1975. The paper states that one of the most widely observed and accepted biological effects of low average power electromagnetic (EM) energy is the auditory sensation evoked in man when exposed to pulsed microwaves.

> That paper's aim was to determine the threshold of the sound-inducing phenomenon as 1) a function of pulse power or energy, pulse shape, and carrier frequency; 2) the locus of the action; that is, whether it is initiated at a central or peripheral site; and 3) whether it is caused by direct action of the EM field on the nervous system or if it activates the auditory system (the ear and related parts that normally conduct sound to the brain).... The threshold for microwave pulse-evoked auditory sensations or responses in both humans and cats is related to the incident energy per pulse, with values of approximately 20 μJ/cm2 for cats to 40 μJ/cm2 for humans for pulses less than 30 μsec wide.
>
> The credit for performing an actual experiment in which audible voices were communicated via microwaves is given to Joseph Sharp and Mark Grove. Sharp is the former director of research in experimental psychology at the Walter Reed Army Institute of Research. Mark Grove, an electronic engineer, put together at Walter Reed what is now one of the best equipped laboratories in the United States for studying biopsychological effects of microwave radiation.

> Judy Wall reports that they recorded on tape the spoken words for the single syllable numbers one through ten. The electrical sine wave analogs of each word was then processed so that each time a sine wave crossed zero reference in the negative direction, a brief pulse of microwave energy was triggered. By radiating themselves with these voice-modulated microwaves, Sharp and Grove were readily able to hear, identify, and distinguish the nine words. The sounds heard were not unlike those emitted by people with artificial larynxes. Communication of more complex words and of sentences was not attempted because the averaged densities of energy required would approach the current 10 mW/cm2 limit of safe exposure.

Those who have seen Frank Sinatra's famous cold-war thriller *The Manchurian Candidate* know that a prime motivation for using mind control is to make unstoppable assassins out of otherwise normal citizens. Regarding this issue, I conclude with a remark from a mind control survivor who is one of the models for *Alice in Americaland*. Here, she speaks of people who commit mass shootings, many of whom seem to have no memory of the actual crime. In addition, many have been under psychiatric care and were taking some form of drugs of a class used by the CIA in mind control programming.

> The one [catchphrase in news accounts] I now watch for is that the perpetrator "was under treatment for depression." I translate this to mean that the person was on Selective Seratonin Re-uptake Inhibitors, such Prozac, Paxil, and Zoloft. You'd be amazed how many news accounts mention this little factor. A little known fact about Patrick Purdy, who shot up a schoolyard in Stockton, California, was that he was on Prozac.

Nearly every mass shooting I have ever examined has also fallen into this category. The most recent was right in my hometown of Springfield, Oregon. Young Kip Kinkel, who had been on Prozac and psychiatric care, was taken off of the treatment. Just a few months later, he killed his parents at home, then went to his school and unloaded his firearms on classmates and teachers, killing two more.

In yet another local incident, a man was arrested for carrying "a small arsenal of loaded weapons and several hundreds of rounds of ammunition" into the shopping center where my wife works. He appeared there again the next day, just as well equipped. Each time, there were curious hate messages scribbled on notes in his pocket, with vague references to "Mother," who "called and told me to..." This man, too, was on Prozac and under psychiatric care. Of course, his mother had not called. Moreover, the hate messages were written, chantlike, in repetition, and they were not aimed at any group or person. Neither were there indicators to suggest that he hated anyone or had any enemies. When questioned, about anything at all, the man simply lost all track of reality and could remember nothing.

All this fits the profile of a Sirhan Sirhan or a subject of mind-control technique. We can see that there is serious reason for concern over this topic. But in the end, you probably won't become prey to mind control unless you have been particularly troublesome. Even so, it might be a good idea not to make any appointments with doctors recommending any of the drugs mentioned here, or with those who suggest hypnotism as part of their treatment program.

Types of Mind Control

In the aftermath of the Korean War, we learned of the early mind-control techniques used on American POWs, which involved sleep deprivation, beatings as negative reinforcement for undesired responses, rewards as positive reinforcement for desired responses, basic mental and physical tortures, and mind games. But unless you are captured by terrorists or groups bearing resemblance to the Symbionese Liberation Army (itself a CIA mind-control project), you probably won't be subjected to that kind of mind control. I would worry more about the more recent flavors.

I view today's mind control as falling into three distinct categories: experiments to advance the science; covert applications for espionage, sabotage, and assassination; and harassment against troublesome targets. The first category has been conducted behind a veil of secrecy, parted now and again to reveal troublesome glimpses into the darkness. The second involves a kind of recruitment of unwilling "participants" who can later be called into play for almost any covert need. The final accounts for anyone who

crosses the intelligence community. In the old days, such a person would just meet with an "unfortunate accident" or suffer a "heart attack." Today, the CIA seems to delight in other, more tortuous solutions to further advance their knowledge.

For mind-control purposes, hapless victims are recruited, and their oppressors create trauma of such intensity as to force the victim into alternate personalities. Multiple personalities fragment the psyche of the victim as a means of dealing with the trauma. For the mind-control programmer, using the right treatment and conditioning provides unique individuals who can be summoned at will. Psychotic personalities who cannot distinguish between right and wrong or who can be programmed to exhibit a perverse enjoyment for inflicting pain can be developed and trained for specific missions. Upon "graduating," the victim leads an ordinary life until being awakened into an alternate identity for action. Afterward, returned to his or her "normal" identity, the victim retains no memory of any vile deed. The only indicators that things may be amiss are lapses in memories and strange dreams, and a steady diet of *deja vu* and general confusion. They are the perfect agent, incapable of betraying secrets and easy to conceal, as there are no ties to the intelligence community or the government. Often, they are used as pawns, expendable agents programmed for assassination.

So it was for Sirhan Sirhan, who was apparently under the care of CIA psychiatrists some years prior to his attack on Robert Kennedy. Thane Cesar, who was associated with the intelligence community and widely believed to be the actual killer, was assigned to a classified operation within Hughes Aircraft, where, once again, ties were found to Sirhan's original psychiatrist.

But harassment via mind-control methods is far more likely than victimization for the purpose of training assassins. Symptoms, which in and of themselves are not concrete evidence, might include mood swings; physical symptoms such as nausea or headaches; unexplained marks or burns on the body; tingling sensations; sleep disorders and nightmares; real-world interactions such as dying plants, televisions which switch on or off or change channels on their own, or unusual interference in radio/television reception; awareness of sounds or voices which can't be heard by others; and ringing in the ears.

Generally, the purpose of harassment is to destroy credibility and make the target appear to be delusional, especially to the media

or the law. In some cases, the goal may be to cause the target to actually go insane or commit suicide. In all cases, the assault is likely to dilute the target's ability to deal with the problems at hand.

Defending Against Mind Control

The best defense is a good offense—but aluminum hats can work, too. A silly statement? Perhaps not. Mind-control techniques involve a fairly straightforward set of principles and procedures. To begin with, a psychological profile is established in order that the victim can be categorized by his weaknesses, which can then be exploited by mental anguish and other artificial pressure. The victim must be under a heavy surveillance net for this purpose. It is believed that EEG (which stands for electroencephalogram, a graphic tracing of the electrical activity of the brain) information is collected in order to establish a "tuned" weapon that will impact upon the victim correctly.

The basic principle here is that the mind generates detectable brain waves that differ depending on what the subject is thinking/doing at the time. Brain-wave patterns can be detected and identified with respect to such things as emotions, or sounds, or visions. This can become useful when applied in reverse. That is, by "broadcasting" the same brain waves back at the target, it is possible to induce a replay of the same emotions, sounds, or visions. Normally, this would require rigid controls and special preparation of the target in order to produce adequate results. However, by continuously bombarding the victim with such material, one can, slowly but surely, impact the victim subliminally. And when the "frequency" of the target is well defined, it is possible to "transmit" words or other sounds directly into their mind. This can be very useful, whether to drive the victim to insanity or to motivate them to act destructively. I have been in contact with a number of people, including former a CIA agent turned Agency critic, who describe an identical pattern of events, symptoms, and apparent strategies related to this technology.

All radio and microwave broadcasts can be detected. Of course, the expense and expertise required can be great—as you've seen in the section regarding Electronic Surveillance–and may be well beyond your reach. However, even an inexpensive TriField Meter described earlier can be useful. Understand that your enemy will need a broadcast position, which should be relatively easy to locate

because it will require at least one, and more likely, two line-of-sight locations. Using two locations, a signal can be split into harmonically sympathetic signals and broadcast from the separate locations to meet again near the target. This ensures that only the target is affected, rather than everyone in the path of a single beam.

Beamed at the target at symmetrical angles of attack (and typically at 45 or 90 degrees to one another), only the area where the broadcasts overlap represents a "hot zone." The overlap will have twice the EMF (Electromagnetic Field) levels of the beam paths. This means that a pattern of frequent tests with such a field strength meter will tell you when you are being attacked, where the danger zones are, and by analysis of the beam paths, where the transmitters are (two possibilities for each beam, when you follow the beam both ways). All you need do is find likely line-of-sight points. This will probably be a building, but it could be anything: a tree, pole, tower, or a structure on a rooftop. The transmitters involved could be the size of a frying pan or a small TV antenna.

If you think you have found the source, you will need a way to discreetly get up close and examine further, preferably when the enemy expects you to be away, such as during work hours. Look for signs of recent installation. If there are wires you can access, and if you can determine which wire is signal (and not power!), you can simply disconnect them and short the lead wire directly to ground (usually the outer woven-wire mesh in coaxial cable, or the only other wire in other types of cable). Try to follow the cable back to its point of origin. If you have trouble isolating it, you can have someone use the field strength meter to monitor the site while you are at home, being "targeted." Even when not your opponents aren't "broadcasting," there will likely be a lot of electronic gear alive and operating within the location, and you'll still be able to get a fix on the signal. If you can locate the source (and even if you cannot defeat the broadcasts), try to set up your own observation post, where you can photograph and identify everyone who comes and goes. When possible, follow them. They just might lead you to someplace interesting. Document everything: time, date, license plates, who, when, where, etc.

APPENDIX I
Additional Reading Materials

The following references several books that offer hope and help from a company called Loompanics. As of this writing, I have not had the time or resources to evaluate the many books they offer in their inch-thick catalog. I suggest that you contact them for a copy of the $5 catalog, which has an in-depth description for each title, or ask their recommendations for books that pertain to your situation. Author information is not always provided in the Loompanics catalog. Books commonly available from public libraries or booksellers are underlined with author information. Libraries are a good source for books on the intelligence community and law enforcement practices.

Loompanics Unlimited
Publishers and Sellers of Unusual Books
P.O. Box 1197
Port Townsend, WA 98368

A Guidebook for the Beginning Sweeper, Glenn H. Whidden/Technical Services Agency (301) 292-6430

Applied Surveillance Photography, Raymond P. Siljander

Ask Me No Questions, I'll Tell You No Lies—How To Survive Being Interviewed, Interrogated, Questioned, Quizzed, Sweated, Grilled...

Big Brother and the Holding Company. A collection of writings supporting the basis for my problems with CIA. Every American needs to know Nixon had a Waco, too—Flight 553!

Big Brother is Listening: Phonetappers & State Security, Duncan Campbell Who needs a court order, anyway?

CIA and the Cult of Intelligence, by Victor Marchetti. An excellent view of the CIA by an ex-agent.

CIA Catalog of Clandestine Weapons, Tools & Gadgets

CIA Flaps & Seals Manual. The art of opening envelopes and seals without detection.

Code Making & Code Breaking

Complete Guide to Lock Picking

The Computer Underground—Hacking, Piracy, Phreaking, & Computer Crime

Cop Talk—Monitoring Law Enforcement Communications

Counterfeit I.D. Made Easy, by Jack Luger

Digital Privacy: A Guide to Computer Privacy, M. L. Shannon

Disguise Techniques, by Edmond A. Macinaugh

The Ear: Volumes I-III, Glenn H. Whidden/Technical Services Agency

Expedient B&E—Tactics For Bypassing Alarms & Defeating Locks

False Profits—The Truth About BCCI. Every American should know how Bush and the CIA ripped them off!

Fatal Rebirth, by H. Michael Sweeney. Describes in detail my problems at the hands of the intelligence community.

Financial Investigations & The Tracing of Funds

Get the Facts on Anyone—How You Can Use Public Sources to Check the Background of Any Person or Organization, by Dennis King

Getaway—Driving Techniques for Escape & Evasion

How to Build a Bug Proof Room

How to Disappear Completely and Never be Found, by Doug Richmond

How to Hide Anything

How to Read Schematics. Lets you build your own electronic devices (bugs, bug detectors, radio devices, scramblers, etc.) from commonly available plans.

How to Use the Federal F.O.I. Act and The Privacy Act of 1974 A citizen's guide to using the Freedom of Information Act and the Privacy Act to request government records.

The Intruders: The Invasion of Privacy by Government and Industry, Edward V. Long

License Plate Book—The Hidden Letter & Number Codes on Plates Unknown to the Public, But Used by Police, by Thomas C. Murray

Lip Reading Made Easy, by Edward B. Nitchie

Manuals on Mayhem—A Complete Guide To The Literature Of Combat, Martial Arts & Serious Self Defense

New I.D. in America—How to Create a Foolproof New Identity

On The Run, by Phillip Agee. Mr. Agee recounts his own flight for freedom from the CIA. Chased around the globe while he wrote this book, Agee exposes illegal CIA operations aimed at manipulation of foreign policy.

Personal & Business Privacy—A Special Report on Why and How Your Privacy is Invaded

Personal Defense Weapons

Psychic Dictatorship in the USA, by Alex Constantine. A whirlwind tour of CIA mind-control projects gone mad.

Plausible Denial, by Mark Lane. The true account of a trial which proves, once and for all, that the CIA killed JFK and that the government has been overthrown by the military-industrial-intelligence complex. Every American should read this book.

Political Trashing

Portfolio of Schematic Diagrams for Electronic Surveillance Devices

Principles of Personal Defense

Shadowing & Surveillance—A Complete Guidebook, by Burt Rapp

Spooks, by Jim Hougan. Great information on all manner of spies and detectives—and their adventures.

SpyCom—Covert Communications Techniques of the Underground

Surreptitious Entry

Take No Prisoners—Destroying Enemies with Dirty & Malicious Tricks

Telephone Eavesdropping and Detection, Richard J. Udovich—a technical TSCM guide

U.S. Attorney's Manual on Electronic Surveillance

The Whole Spy Catalog, James Bamford

Winning the IRS Game—How anyone can beat the IRS

Wiretapping & Electronic Surveillance—Federal Government Commissioned Studies

APPENDIX II

CIA-Related Organizations

This section includes a sampling of the many CIA proprietaries in existence. Jim Hougan, author of the excellent *Spooks*, estimates that as far back as 1966 there were over 100 industrial security firms headed by former FBI or CIA officers, all of which likely shared favors with their old employers—and this was just one small private-sector market into which intelligence operatives moved once they retired. He also points out that, today, many Fortune 500 companies hire retired intelligence types, as do many of the nation's wealthiest families (think Rockefeller, Hunt, Getty, DuPont, etc.) looking for specialty personal protection and other services. Also, there are hundreds of college professors and even entire university departments or research institutes regularly performing tasks for the CIA, including recruiting.

The list also includes those engaged in financial rape and other profiteering by illegal activities involving machinations of these same intelligence elements—a kindred in conspiratorial activities that Daniel Sheehan of the Christic Institute called the "Secret Team." For a better understanding of these fronts, consult *Spooks* and Jonathan Kwitney's *The Crimes of Patriots*, which detail how the fronts are tied not only to the intelligence community but to elite power players internationally, including the Council on Foreign Relations, the Trilateral Commission, and the Bilderbergers. I encourage you to consider these groups carefully, given the undue influence they seem able to exert on our nation's intelligence community. (Then again, the argument could be made that these groups essentially birthed the modern intelligence community).

With respect to the names listed below, note the wide diversity and odd mix of naming conventions—you can't usually tell these books by their cover. Inclusion on the list is not, in and of itself, concrete proof of CIA affiliation, but rather an indication that, at the least, its leadership has, at one time, operated within spheres of Agency influence. Some may even be counted as "good guys" for that relationship, as they may have served or may be serving legitimate national security interests, and may even be doing so openly (as is the case with the contractors found here). Interestingly, I have had over a dozen names submitted to me for inclusion on the list by employees themselves. I have not included any names on that basis alone; I always ask for a reasonable basis or justification for inclusion.

As a final note, it is ironic, perhaps, that the bulk of the fronts listed which are still active entities are spin-offs of CIA mind-control projects. Thus, while the CIA and so-called experts claim that the CIA ended mind-control experiments in the 70s, someone has found a reason to continue in the field. Indeed, projects affiliated with the Cult Awareness Network seem to be busy working with mind-control technologies, while others, tied to the False Memory Syndrome Foundation, seem bent on disproving that these technologies are even possible—a built-in plausible denial. Laughably, some of the principle players drifting in and out of CAN, FMSF, and the original MK Ultra experiments are often the same people, and these groups often work together.

CIA Proprietaries, CIA Infiltrated or Influenced Organizations, and CIA Contractors/Suppliers of Intelligence equipment:

AAI Corporation (Supplier): James M. Atkinson, Granite Island Group

Actus Technology: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Aero Associates (suspected to be involved in illegal CIA foreign weapons sales): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

AFF News (publication of AFF): AFF materials—see also ICEP

Agency for International Development (shared facilities with NIA): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Air America: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Air Asia: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

All Saints Lutheran Church (Bowie, Maryland—CAN and FMSF ties): ICEP materials

Allen Memorial Institute (Montreal—mind-control projects)

AlliedSignal, Inc. (Supplier): James M. Atkinson, Granite Island Group

American Committee for Liberation (of Cuba): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

American Committee on a United Europe: Jim Hougan, *Spooks*

American Council of Churches (established by Howard Hunt): Torbitt document, Internet

American Enterprise Institute (CIA propaganda factory used by FMSF)

American Family Foundation: Daniel Brandt, *Namebase Newsline*

American Institute of Hypnosis (Dr. William Bryan, MK Ultra, believed to have programmed Sirhan Sirhan): Alex Constantine, *Psychic Dictatorship in the USA*

The American Institutes of Research: Alex Constantine, *Mind Control Operations at Stanford Research Institute*

American Psychiatric Association (headed by CIA mind-control experimenter, Dr. Ewen Cameron): Alex Constantine, *Psychic Dictatorship in the USA*

Americares: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*, Summer '92 issue (Exposes George Bush family financial ties to intelligence community and criminals)

Anderson Security Associates (Virginia): Jim Hougan, *Spooks*

API Distributors, Inc. (A Houston firm involving famous spooks Richard Secord, Thomas Clines, Ted Shackley): Jonathan Kwitney, *The Crimes Of Patriots*; David Corn, *The Blond Ghost*

Appalachian State University (CAN and FMSF ties): ICEP materials

Arbusto Energy, Inc.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Armairco (Oliver North Iran-Contra): John Prados, President's Secret Wars

Arnim Proprietary, Ltd.: Jonathan Kwitney, *The Crimes of Patriots*

Arthur D. Little (hires retired spooks in quantity): Jim Hougan, *Spooks*

Asia Foundation: Jonathan Kwitney, *The Crimes of Patriots*

Asset Management International Financing & Settlement Ltd.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Association of College Unions-International (ACU-I—CAN and FMSF ties): ICEP materials

Association of Former Intelligence Officers (AFIO): Mark Lane, *Plausible Denial*; Jim Hougan, *Spooks*

AT&T Federal Systems Advanced (Supplier): James M. Atkinson, Granite Island Group

Audio Intelligence Devices, Inc. (Ft. Lauderdale—associated with NIA): Jim Hougan, *Spooks*

Austin Society to Oppose Pseudoscience (ASTOP—CAN and FMSF ties): ICEP materials

Australian Association for Cultural Freedom: Jonathan Kwitney, *The Crimes of Patriots*

Autometric, Inc. (Supplier): James M. Atkinson, Granite Island Group

B.R. Fox Laboratories (B.R. Fox Company): Jim Hougan, *Spooks*

BAC International Credit Corp. (Contra Resupply/Money Laundering): John Semien, "Congress Investigating Barry Seal's Activities," *Baton Rouge Sunday Advocate*

Bagwhan Shree Rajneesh Movement (El Salvador CIA ops ties and MK Ultra spin off) Ace Hayes, *Ace Hayes Secret Government Seminar*

Bahamas Commonwealth Bank (Vesco/IOS company): Jim Hougan, *Spooks*

Bank of Credit and Commerce International (BCCI): Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Bass Enterprises Production Company: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Battelle Memorial Institute and other Battelle operations (hires retired spooks in quantity): Jim Hougan, *Spooks*

Beth Israel Hospital (FMSF involvement): FMSF materials

Biblical and Theological Studies, Gordon College (Wenhans, Massachusetts—CAN and FMSF ties): ICEP materials

Bird Air (the infamous William "Wally" Bird): Jonathan Kwitney, *The Crimes Of Patriots*

Bishop, Baldwin, Rewald, Dillingham and Wong (Hawaiian local family names of good repute usurped for financial swindles and other CIA benefit): Jonathan Kwitney, *The Crimes Of Patriots*

Boeing Company (Supplier): James M. Atkinson, Granite Island Group

Booz, Allen & Hamilton, Inc. (Intelligence Contractor): John Pike, American Federation of Scientists

Boston City Hospital (mind control related): Alex Constantine, *Psychic Dictatorship in the USA*

Boston Psychopathic Hospital: John Marks, MK Ultra Behavior Control Experiments Document Collection

Boston University, Marsh Chapel (CAN and FMSF ties): ICEP materials

Bothell Washington Schools (high-school counseling CAN and FMSF ties): ICEP materials

Broward Federal Savings and Loan: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Bruce Campbell and Company: Jonathan Kwitney, *The Crimes Of Patriots*

Bureau of Applied Social Research (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

California Microwave, Inc. (Supplier): James M. Atkinson, Granite Island Group

Canadian Psychiatric Association (headed by CIA mind-control experimenter, Dr. Ewen Cameron): Alex Constantine, *Psychic Dictatorship in the USA*

Caramar (Caribbean Marine Aero Corp.): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Carnegie Foundation (CIA project funding): Daniel Brandt, Namebase Newsline

Carnegie Mellon University (Social/Decision Sciences dept.—FMSF involvement): FMSF materials

CAS, Inc. (Supplier): James M. Atkinson, Granite Island Group

Castle Bank and Trust (ties to both Robert Vesco and his junior in CIA financial swindles, Nugan Hand): Jonathan Kwitney, *The Crimes Of Patriots*

Castle Bank and Trust, Ltd.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

CBS (collusion with CIA to destroy Jim Garrison, access to CIA vote-fixing information, pattern of CIA-friendly newscasting and cover-ups): James M. Collier and Kenneth F. Collier, "Votescam: the Stealing of

America"; Interview with Jim Garrison, *Playboy*

Center for International Studies at MIT (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

Center for Sexuality and Religion (FMSF ties)

Central Agency for Jewish Education (Miami high-school counseling CAN and FMSF ties): ICEP materials

Central America Freedom Program: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Central Investigative Agency: Jim Hougan, *Spooks*

Century Special (controlled by ICC): Jim Hougan, *Spooks*

Chalk's International Airlines (Vesco/IOS company): Jim Hougan, *Spooks*

Charing Cross Hospital (Psychiatry dept.—FMSF involvement): FMSF materials

Cherry Creek National Bank: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Church League of America (shares intelligence dossiers on American citizens with CIA proprietaries): Jim Hougan, *Spooks*

Citizens Freedom Foundation (predecessor to Cult Awareness Network): Daniel Brandt, *Namebase Newsline*

City University of New York, Graduate School (CAN and FMSF ties): ICEP materials

Civil Air Transport: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Civilian Irregular Defense Group(s): John Prados, *President's Secret Wars*

Civilian Military Assistance (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

CMI Investments (evolved into Bishop, Baldwin, Rewald, Dillingham and Wong): Jonathan Kwitney, *The Crimes Of Patriots*

Cocke and Phillips International (Nugan Hand's direct link to Intelligence in Washington D.C.): Jonathan Kwitney, *The Crimes Of Patriots*

College of Foreign Affairs, University of Indiana

Colleyville Texas Schools (high-school counseling CAN and FMSF ties): ICEP materials

Colorado State University (CAN and FMSF ties): ICEP materials

Columbia University (high-school counseling CAN and FMSF ties): ICEP materials

Commission on Cults and Missionaries, Jewish Federation Council of Greater Los Angeles (CAN and FMSF ties): ICEP materials

Committee for Scientific Examination of Religion

Committee for Scientific Examination of Claims of the Paranormal

Committee for the Defense of National Interests: John Prados, *President's Secret Wars*

Committee of One Million Against the Admission of Communist China to the United Nations: John Prados, *President's Secret Wars*

Comptrol International (Vesco/CIA/arms smuggler partners): Jim Hougan, *Spooks*

Concordia University (Quebec—Psychology dept.—FMSF involvement): FMSF materials

Condor Systems (Intelligence Contractor): John Pike, *American Federation of Scientists*

Congress for Cultural Freedom: Daniel Brandt, *Namebase Newsline*

Consultants International (formerly Maritime Consulting): David Corn, *The Blond Ghost*

Coordination of United Revolutionary Organizations: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Cornell University, Human Ecology Fund

Cornell University, Registrars Office (CAN and FMSF ties): ICEP materials

Cornell University, Society for the Investigation of Human Ecology: Alex Constantine, *Psychic Dictatorship in the USA*

Corporate Air Services (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Corporate Training Unlimited (mind-control related): Alex Constantine, *Psychic Dictatorship in the USA*

COSECOIN (Corporate Security Consultants International): Jim Hougan, *Spooks*

Council on Foreign Relations (CIA bedfellow or, as this work suggests, CIA controller): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Crest Detective Agency (Santa Monica): Jim Hougan, *Spooks*

Cryogenics, Inc. (controlled by Robert Vesco): Jim Hougan, *Spooks*

Cuban American National Foundation: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Cult Awareness Network—MK Ultra offspring infiltrates legitimate church groups, involved in shaping early religious paths of Reverend Jim Jones and David Koresh) Ace Hayes, *Ace Hayes Secret Government Seminar*

Cult Hot Line and Clinic, Jewish Board of Family and Children's Services: AFF materials—see also ICEP

Cult Resource Center, Ecumenical Ministries of Oregon: AFF materials—see also ICEP

Cultic Studies Journal (publication of AFF): AFF materials—see also ICEP

Dallas Western Savings Association: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

David Sarnoff Research Center (Intelligence Contractor): John Pike, *American Federation of Scientists*

Defense Services, Inc.: Jim Hougan, *Spooks*

Defense Systems, International: Jim Hougan, *Spooks*

Dektor Counterintelligence (Virginia): Jim Hougan, *Spooks*

Delfin Systems (Intelligence Contractor): John Pike, *American Federation of Scientists*

Denver University: John Marks, MK Ultra Behavior Control Experiments Document Collection

Diamond Shamrock Corp. (provided male prostitutes for CIA political blackmails): Alex Constantine, *Psychic Dictatorship in the USA*

Directorate of Science and Technology (conduit for CIA work with professors, university departments, and research organizations): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Double Day and Company (Publisher—knowingly published fraudulent CIA books): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Double-Check Corporation: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Draper-JSC (Supplier): James M. Atkinson, Granite Island Group

Drew Pearson (reporter, regularly debriefed by CIA): Victor Marchetti, John D. Marks, *The CIA and the Cult of Intelligence*

Eagle Aviation Technology and Services (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Eastman Kodak Company (Intelligence Contractor): John Pike, *American Federation of Scientists*

EATSCO (the Egyptian American Transport and Service Company): Daniel Sheehan, *The Secret Team*

Ecumenical Ministries of Oregon, Cult Resource Center: AFF materials—see also ICEP

EG&G, Inc. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Electrical Construction (Portland—alternating name in Yellow Pages for local front): Harry Sweeney, *Fatal Rebirth*

Electrical Contractors (Portland—alternating name in Yellow Pages for local front): Harry Sweeney, *Fatal Rebirth*

Emory University (Psychiatry dept.—FMSF involvement): FMSF materials

Encounter (academic journal): Alex Constantine, *Psychic Dictatorship in the USA*; Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Energy Resources (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

ESI (Electronic Specialties, Inc.—a Portland area firm controlled by ICC): Jim Hougan, *Spooks*; Eric Mason, KION TV news reporter, doing background research on CIA proprietaries and PAMCO scandal

Evergreen International Air (deleted from Victor Marchetti's book by Government censors): Oregonian; John Prados, *President's Secret Wars*; Eric Mason, KION TV news reporter, doing background research on CIA proprietaries and PAMCO scandal

Experimental Psychiatry Laboratory, University of Pennsylvania

Export Control Systems: Jim Hougan, *Spooks*

Exxon (unnamed subsidiary created by Venezuelan merger of unnamed CIA front with local Exxon subsidiary): Jim Hougan, *Spooks*

FACTnet (headed by former CAN leadership): H. Michael Sweeney, *Alice in Americaland*

Fairfield Aviation (controlled by ICC): Jim Hougan, *Spooks*

False Memory Syndrome Foundation (Counters mind control claims by victims, effectively denying MK Ultra operational results)

Farsight Institute (UFO and mind control related): Alex Constantine, *Mind Control Operations at Stanford Research Institute*

FGM, Inc. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Fidelity Reporting Service (covert background checks on Americans): Jim Hougan, *Spooks*

Fiduciary Trust Company (Stepchild of IOS): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Field Foundation: Ralph McGehee, *CIA Namebase*

Financial General Bankshares: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Finders (MK Ultra spin off where CIA acquires children for unknown purposes—see also Seekers): Daniel Brandt, *Namebase Newsline*

First American Bankshares: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

First Congressional Church (Fairhaven, Connecticut—CAN and FMSF ties): ICEP materials

Ford Foundation (CIA project funding): Daniel Brandt, *Namebase Newsline*

Foreign Broadcast Information Service (monitors radio broadcasts, even of U.S. commercial stations): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Framingham State College, Student Services (CAN and FMSF ties): ICEP materials

Fredrick A. Praeger (Publisher—published CIA favorable books at agency request): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Functional Devices, Inc. (Russiaville, IN): Jim Hougan, *Spooks*

Fund For Peace (headed by spooks): Jim Hougan, *Spooks*

GEICO (Government Employees Insurance Company—provided NIA with contributions), Jim Hougan, *Spooks*

Geneva's Exchange and Investment Bank (Vesco controlled): Jim Hougan, *Spooks*

George L. Barnes & Associates (Los Angeles): Jim Hougan, *Spooks*

Georgetown University Hospital: John Marks, MK Ultra Behavior Control Experiments Document Collection; Alex Constantine, *Psychic Dictatorship in the USA*

Gerschickter Foundation (funded CIA mind control projects): Alex Constantine, *Psychic Dictatorship in the USA*

Gibraltar Steamship Corp.: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Glendale California Schools (high-school counseling CAN and FMSF ties): ICEP materials

Global Financial (Vesco operation): Jim Hougan, *Spooks*

Golden West Airlines (controlled by ICC): Jim Hougan, *Spooks*

Good International, Inc.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Gordon College, Biblical and Theological Studies (Wenhans, MA—CAN and FMSF ties): ICEP materials

Graduate School of Education, University of Pennsylvania (CAN and FMSF ties): ICEP materials

Graduate School, City University of New York (CAN and FMSF ties): ICEP materials

Grand Bahama Development Company (Vesco operation): Jim Hougan, *Spooks*

Gray and Company (Public Relations firm working with CIA against American Citizens—Oliver North Iran-Contra): John Prados, *President's Secret Wars*, Alex Constantine, *Psychic Dictatorship in the USA*

GRC International, Inc. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Great American Banks (drug money laundering): Jonathan Kwitney, *The Crimes Of Patriots*

GTE Government Sector Corp. (Intelligence Contractor): John Pike, *American Federation of Scientists*

GTE Government Systems Corporation (Supplier): James M. Atkinson, Granite Island Group

Gulf Stream, Ltd. (Vesco operation): Jim Hougan, *Spooks*

Gulfstream Land and Development: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Harken Energy Corporation: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Harper and Row, Inc. (publishers, submitted books critical of CIA to CIA for review and censorship prior to publishing): Victor Marchetti, John D. Marks, *The CIA and the Cult of Intelligence*

Harpoon Harry's (CIA spying on US military on R&R): Jonathan Kwitney, *The Crimes Of Patriots*

Harris Corporation, Electronic Systems Sector (Supplier): James M. Atkinson, Granite

Harris Corporation, Harris Semiconductor (Intelligence Contractor): John Pike, *American Federation of Scientists*

Harrison Salisbury (reporter, regularly debriefed by CIA): Victor Marchetti, John D. Marks, *The CIA and the Cult of Intelligence*

Harvard University (Psychology/psychiatric depts.—FMSF involvement): FMSF materials

Harvard University's Center for International Affairs (files contained minutes of Council on Foreign Relations meetings involving CIA operatives addressing National Security matters): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Hercules Research Corporation (METC Unit bomb development): Michael Reconoscuito, Ted L. Gunderson, others

Hill & Knowlton (Public Relations firm used for CIA disinformation campaigns against American citizens): John Carlisle, Public Relationships: Hill & Knowlton, *Robert Gray, and the CIA*, Spring 1993 issue of *CAQ*; Alex Constantine, *Psychic Dictatorship in the U.S.*

Hogan & Hartson, legal firm (Edward Bennett Williams firm): Jim Hougan, *Spooks*

Holmesburg Prison (MK Ultra spin off—involved U. of Penn.)

Honeywell (pursued mind control technology): Alex Constantine, *Psychic Dictatorship in the USA*

Howard Hughes Medical Institute (includes CIA hospital for plastic surgery and other covert operations, literal and figurative, where Evergreen flew both Shah of Iran and Howard Hughes in their last days): Jim Hougan, *Spooks*

Hughes Corporation, Glomar Explorer (CIA project to retrieve sunken Soviet nuclear missiles): Jim Hougan, *Spooks*

Hughes Electronics (Supplier): James M. Atkinson, Granite Island Group

IBM (International Business Machines—IBM executives stated they consider themselves an extension of the federal government, all IBM mainframes have back-door accesses available to government, IBM hires large quantities of CIA): Jim Hougan, *Spooks*

IBM Government Systems (Intelligence Contractor): John Pike, American Federation of Scientists

ICC (International Controls Corp.—controlled by Robert Vesco): Jim Hougan, *Spooks*

Idea, Incorporated (Oliver North's Contra assistance cover): Daniel Sheehan, *The Secret Team*

Impossible Electronic Techniques (Russiaville, IN): Jim Hougan, *Spooks*

Indiana University (Linguistics/Semiotics depts.—FMSF involvement): FMSF materials

Info-Cult (Montreal—CAN and FMSF ties): ICEP materials

Information Council of the Americas (mind control related): Alex Constantine, *Psychic Dictatorship in the USA*

Institute for Social Research, University of Michigan (intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

Institute of Pennsylvania Hospital, University of Pennsylvania (Psychology/Psychiatric depts.—FMSF involvement): FMSF materials

Institute of Psychological Therapies (Psychology dept.—FMSF involvement): FMSF materials

Intelligence Research: David Corn, *The Blond Ghost*

Intelectron Corp. (MK Ultra mind control): Alex Constantine, *Psychic Dictatorship in the USA*

Inter-American Capital (Vesco operation): Jim Hougan, *Spooks*

Inter-Probe, Inc. (METC Unit bomb development): Michael Riconosciuto, Ted L. Gunderson, others

Interarmco (International Armament Corp.): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Intercontinental Industries (controlled by ICC): Jim Hougan, *Spooks*

Interfaith Coalition of Concern About Cults (NY—CAN and FMSF ties): ICEP materials

Intermountain Aviation: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

International Bancorp, Ltd. (Vesco/IOS company): Jim Hougan, *Spooks*

International Business Communications (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

International Campaign for Tibet: Ralph McGehee, *CIA base*

International Committee of Red Cross (ICRC): Ralph McGehee, *CIA base*

International Credit Bank of Switzerland (headed by WWII intelligence operative with more ties to Mossad and Bilderbergers than CIA, but worked closely with Vesco and IOS): Jim Hougan, *Spooks*

International Cult Education Program (ICEP—CAN and FMSF ties): ICEP materials

International Cult Education Program (ICEP): ICEP materials—see CAN, AFF

International Investigators, Inc. (started by Robert Peloquin, presumed architect of the Three I's and Five I's project portrayed in my upcoming book, *Fatal Rebirth*): Jim Hougan, *Spooks*

International Medical Centers: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

International Police Services (INPOLSE—an NIA equivalent dealing more with foreign law enforcement agencies): Jim Hougan, *Spooks*

International Research and Trade Corporation (later became EATSCO): Daniel Sheehan, *The Secret Team;* David Corn, *The Blond Ghost*

Intertel (International Intelligence Incorporated started by Robert Peloquin, possible architect of the Three I's and Five I's project portrayed in this book), Jim Hougan, *Spooks*

IntrAmerica Investments: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Investair Leasing (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

IOS (Investor's Overseas Services—prone to investing client moneys into nefarious CIA projects—later "looted" by Robert Vesco): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Iowa State Hospital: John Marks, MK Ultra Behavior Control Experiments Document Collection

ITT (International Telephone and Telegraph—collusion with CIA to destroy South American governments and take over telecommunications systems): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

J.G. Van Dyke & Associates (VDA—Intelligence Contractor): John Pike, *American Federation of Scientists*

James Martin Government Intelligence (JMGI—Intelligence Contractor): John Pike, *American Federation of Scientists*

Jamestown Community College (Sociology dept.—FMSF involvement): FMSF materials

Jewish Board of Family and Children's Services, Cult Hot Line and Clinic: AFF materials—see also ICEP

Jewish Community Relations Council of New York, Task Force on Missionaries and Cults (CAN and FMSF ties): ICEP materials

Jewish Federation Council of Greater Los Angeles, Commission on Cults and Missionaries (CAN and FMSF ties): ICEP materials

JNB Exploration Company: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

John Hopkins Memorial Hospital (mind control related, FMSF ties): Alex Constantine, *Psychic Dictatorship in the USA*

John Hopkins University (Psychiatry dept.—FMSF involvement): FMSF materials

John P. Muldoon Detective Agency (Katherine Graham's preferred agency): Jim Hougan, *Spooks*

Jonestown (People's Temple—ties to MK Ultra operatives): Daniel Brandt, *Namebase Newsline*

Joseph Alsop (reporter, regularly debriefed by CIA): Victor Marchetti, John D. Marks, *The CIA and the Cult of Intelligence*

Joseph Z. Taylor & Associates (Drug smuggling—documents CIA agents being busted with 50 lbs. of drugs but released with drugs at CIA request): Jim Hougan, *Spooks*

Journal of Defense and Diplomacy (CIA disinformation source): David Corn, *The Blond Ghost*

Kennametal Corp. (covert sales of arms to Iraq involving Hillary Clinton): *American Spectator*, Nov. 96

Kenyon Electronics (controlled by ICC): Jim Hougan, Spooks

Kilmory Investments, Ltd. (Vesco/IOS bedfellow): Jim Hougan, *Spooks*

Lafarge Corp. (covert sales of arms to Iraq involving Hillary Clinton): *American Spectator*, Nov. 96

Lake Resources (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Laurentian University (Psychology dept.—FMSF involvement): FMSF materials

Law Enforcement Assistance Administration (Federal agency rich with CIA operative—influential in local law enforcement): Jim Hougan, *Spooks*

Law Enforcement Intelligence Unit (fraternity of cops who have attended NIA): Daniel Sheehan, *The Secret Team*

Lee Thomas Careers, Inc. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Linking Progressive Corp., S.A. (Vesco operation): Jim Hougan, *Spooks*

Litton Industries, Inc. (Supplier): James M. Atkinson, Granite Island Group

Lockheed (Operation PANDOR mind control subcontractor, employer of Thane Cesar): Alex Constantine, *Psychic Dictatorship in the USA*

Lockheed-Martin Missiles and Space (Supplier): James M. Atkinson, Granite Island Group

Look Magazine (made changes in articles from republished works critical of CIA at CIA direction): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Lotus Development Corp. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Magnavox (Supplier): James M. Atkinson, Granite Island Group

Management Safeguards, Inc. (New York): Jim Hougan, *Spooks*

Mankind Research Unlimited (Wash. D.C.—mind control related): Alex Constantine, *Psychic Dictatorship in the USA*

Maritime Consulting Associates (became Consultants International): David Corn, *The Blond Ghost*

Marsh Chapel, Boston University (CAN and FMSF ties): ICEP materials

Massachusetts Institute of Technology, Center for International Studies (funded by CIA and prepared CIA backed think-tank reports): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

McCord Associates (of Watergate fame, with offices in Maryland and Houston—George Bush's stomping grounds): Jim Hougan, *Spooks*

McDonnell Douglas Aerospace (Supplier): James M. Atkinson, Granite Island Group

McGill University (mind control projects): Alex Constantine, *Psychic Dictatorship in the USA*

MCQ Associates, Inc. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Mercantile Bank and Trust Company: Jonathan Kwitney, *The Crimes Of Patriots*

Meridian Arms (METC Unit bomb development): Michael Reconoscuito, Ted L. Gunderson, others

Miami Daily News (employed Nobel Prize winner and known friend of CIA, Hal Hendrix, who wrote articles using CIA supplied information): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Michigan State University, School of Police Administration: David Corn, *The Blond Ghost*

Military Armaments Corp. (Ingram machine gun "MAC-10" mfg.): Jim Hougan, *Spooks*

MIT Center for International Studies (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

MITRE Corporation (hires retired spooks in quantity): Jim Hougan, *Spooks*

Monsanto (CIA involved corporate leadership): Alex Constantine, *Psychic Dictatorship in the USA*

Moral Re-Armament: Daniel Brandt, Namebase Newsline; Alex Constantine, *Psychic Dictatorship in the USA*

MOVE (MK Ultra spin off—Philadelphia headquarters firebombed by Police helicopters)

Mt. Sinai School of Medicine (Psychiatry dept.—FMSF involvement): FMSF materials

Mystech Associates, Inc. (Supplier): James M. Atkinson, Granite Island Group

National Association of Intelligence Officers (retired intelligence association serves intelligence interests): David Corn, *The Blond Ghost*

National Association of Student Personnel Administrators (NASPA—CAN and FMSF ties): ICEP materials

National Commission on Marijuana and Drug Abuse (operation of hit-squads to assassinate competing drug lords): Jim Hougan, *Spooks*

National Committee for a Free Europe: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

National Endowment for Democracy: Daniel Brandt, *Namebase Newsline*

National Endowment for the Preservation of Liberty (Oliver North Iran-Contra—not truly a front, but operated for CIA benefit): John Prados, *President's Secret Wars*

National Institute of Health (mind control experiments): Alex Constantine, *Psychic Dictatorship in the USA*

National Intelligence Academy, (NIA, now believed to be the Liddy Institute), Jim Hougan, *Spooks*, H. Michael Sweeney, *Fatal Rebirth*

National Opinion Research Center (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

National Railways Security Bureau, Inc.: Jim Hougan, *Spooks*

National Social Democratic Front: David Corn, *The Blond Ghost*

National Student Association (funded by CIA): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

New World Publishing (disinformation book mill): David Corn, *The Blond Ghost*

New York Times (collusion with CIA to cover up CIA crimes, CIA friendly reporting, knowingly publishing CIA supplied articles containing slander without confirming facts): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*, others

Newman Center, University of Pennsylvania (CAN and FMSF ties): ICEP materials

Newsweek (willingly published CIA promotional and disinformation articles): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Norman Jaspen & Associates: Jim Hougan, *Spooks*

Northrop Grumman Corp. (Supplier): James M. Atkinson, Granite Island Group

Northwest Federal Credit Union (CIA employees credit union): John Pike, *American Federation of Scientists*

Nugan Fruit Group (Drug operations): Jonathan Kwitney, *The Crimes Of Patriots*

Nugan Hand Bank (Principle arm of CIA's Michael Hand swindles and drug operations): Jonathan Kwitney, *The Crimes of Patriots*

Oceanic Bank (S.F.—Marcos/CIA joint venture): Alex Constantine, *Psychic Dictatorship in the USA*

Olin Foundation (CIA funding cover)

Omni Spectra, Inc. (Tempe, AZ): Jim Hougan, *Spooks*

Orange Spot (Soft drink company used for money laundering): Jonathan Kwitney, *The Crimes Of Patriots*

Order of the Temple of Astarte (MK Ultra spin off—Pasadena)

Oregon Health Sciences University (Psychology dept.—FMSF involvement): FMSF materials

Overseas Southeast Asia Supply Company (Sea Supply): John Prados, *President's Secret Wars*

Pacific Architects and Engineers: Alex Constantine, *Psychic Dictatorship in the USA*

Pacific Corporation: Victor Marchetti/John D. Marks, The CIA and the Cult of Intelligence; John Prados, *President's Secret Wars*

Pacific-Sierra Research Corp. (Intelligence Contractor): John Pike, *American Federation of Scientists*

Palmer National Bank: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

PAMCO (Pacific Aircraft Maintenance Company—$60M swindle involving Pacific Corp. and Evergreen Aviation. Site now operating as "AMC" with considerable secrecy.) Oregonian; Harry Sweeney, *Fatal Rebirth*

Pan Aviation (Miami): Bradley Ayers, WPLG-TV reporting on CIA drug smuggling

Paradise Island Casino (Vesco operation with exotic partners in organized crime, religious leaders, and presidential bedfellows—where this author played a single $5 roulette bet and, upon wining, let it ride to win again): Jim Hougan, *Spooks*

Pellow Wease Chemical Co.: John Marks, MK Ultra Behavior Control Experiments Document Collection

People's Temple (Jonestown—ties to MKULTRA operatives): Daniel Brandt, *Namebase Newsline*

Peoples State Bank: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Philip M Stern Foundation: Ralph McGehee, *CIA Namebase*

Phoenix Financial (Vesco operation): Jim Hougan, *Spooks*

Pinellas County Schools (high-school counseling CAN and FMSF ties): ICEP materials

Polaroid Corporation (Dr. Land funded SEI and supervised U-2 projects)

Popular Bank of Hialeah (Contra Resupply/Money Laundering): John Semien, "Congress Investigating Barry Seal's Activities," *Baton Rouge Sunday Advocate*

Prescott Bush & Co.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Prescott Bush Resources Ltd.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Price Waterhouse (not a true front, but certified obviously fraudulent books for CIA fronts): Jonathan Kwitney, *The Crimes Of Patriots*

Project Democracy (Oliver North Iran-Contra): John Prados, *President's Secret Wars*, Jim Hougan, *Spooks*

Property Resources, Ltd. (Vesco operation): Jim Hougan, *Spooks*

Psychiatry and Biobehavioral Sciences at UCLA's School of Medicine: Daniel Brandt, *Namebase Newsline*

Psychology in Education Division, University of Pennsylvania (CAN and FMSF ties): ICEP materials

Quantum Corp. (not the hard drive maker): Jim Hougan, *Spooks*

Radio Americas: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Radio Free Asia: Offspring of the Radio Free Europe, Radio Americas, *Radio Liberty*

Radio Free Europe: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Radio Liberty: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Radio Swan: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

RAND Corporation (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

Rapid-American Corp. (Vesco-IOS related): Jim Hougan, *Spooks*

Raytheon (Supplier): James M. Atkinson, Granite Island Group

Red Cross (infiltrated as cover agency for international operations): Ralph McGehee, *CIA Namebase*

Red Pearl Bay, S.A. (Vesco operation): Jim Hougan, *Spooks*

Research Associates International (RAI): David Corn, *The Blond Ghost*

Research Associates of Syracuse, Inc. (RAS) (Supplier): James M. Atkinson, Granite

Resorts International (Parent of Intertel): Jim Hougan, *Spooks*

Rice University (Psychology dept.—FMSF involvement): FMSF materials

Ridgeview Center for Dissociative Disorders (FMSF involvement): FMSF materials

Robert A. Maheu Associates (of Howard Hughes fame): Jim Hougan, *Spooks*

Robert R. Mullen Company (Howard Hughes funded, CIA operated): Len Colodny, Robert Gettlin, Silent Coup

Robert Wood Johnson Medical Center (Psychiatry dept.—FMSF involvement): FMSF materials

Rockefeller Foundation (CIA project funding, including mind control): Daniel Brandt, *Namebase Newsline*, Alex Constantine, *Psychic Dictatorship in the USA*

Rockwell International Corporation (Supplier): James M. Atkinson, Granite Island Group

Rohde and Schwarz (Supplier): James M. Atkinson, Granite Island Group

Roman Catholic Archdiocese of NY (CAN and FMSF ties): ICEP materials

Rush Presbyterian St. Luke's Medical Center (Sleep Disorder Center—FMSF involvement): FMSF materials

Rutgers, Forum for Policy Research

Sacramento California Schools (high-school counseling CAN and FMSF ties): ICEP materials

SAIC (Supplier): James M. Atkinson, Granite Island Group

Santa Elena (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

School of Police Administration, Michigan State University: David Corn, *The Blond Ghost*

Scientific Engineering Institute (SEI—Boston & University of S. Carolina, U. of Penn—Operation Often Chick-Wit, spin off of MK Ultra devoted to witchcraft, demonology, and voodoo)

Scientology (infiltrated/manipulated): Daniel Brandt, Namebase Newsline, Alex Constantine, *Psychic Dictatorship in the USA*

Seafarer's International Union of North America

SECOIN (Security Consultants International): Jim Hougan, *Spooks*

Seekers (MK Ultra spin off where CIA acquires children for unknown purposes—see also Finders): Daniel Brandt, *Namebase Newsline*

Service Observance Bureau of The Bell System (conducts unregulated wiretaps of clients—175,000 in Manhattan alone in one year—shared freely with intelligence community): Jim Hougan, *Spooks*

Seton Hall University (South Orange, NJ—CAN and FMSF ties): ICEP materials

Sex Information and Education Council (FMSF ties)

Sheffield Edwards & Associates (Virginia): Jim Hougan, *Spooks*

Shenandoah Air Leasing (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Siemens Corporation (Supplier): James M. Atkinson, Granite Island Group

Silverado Banking Savings and Loan: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

SIONICS (Ingram machine gun developer): Jim Hougan, *Spooks*

Smith-Richardson Foundation (CIA project funding): Daniel Brandt, *Namebase Newsline*

Society for the Investigation of Human Ecology, Cornell University: Alex Constantine, *Psychic Dictatorship in the USA*

Soldier of Fortune (started by intelligence types and heavy employer of former intelligence types—walks the fine line of exposing and protecting intelligence criminal activities): Jim Hougan, Spooks; Alex Constantine, *Psychic Dictatorship in the USA*

Southern Air Transport: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Spectre Security Products (Orange, CA): Jim Hougan, *Spooks*

Spectrum 7 Energy Corporation: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

SRI International (Intelligence Contractor): John Pike, *American Federation of Scientists*

SSDS, Inc. (Intelligence Contractor): John Pike, *American Federation of Scientists*

St. Elizabeth's Hospital (Bethesda—mind control related): Alex Constantine, *Psychic Dictatorship in the USA*

St. Johns Episcopal Church (Carlisle, Penn.—CAN and FMSF ties): ICEP materials

St. Lucia Airways (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Standard Commerz Bank of Switzerland (Vesco controlled): Jim Hougan, *Spooks*

Stanford Research Institute. (Stanford University—Intelligence Contractor): John Pike, *American Federation of Scientists*

Stanford Technology Trading Group International (STTGI—Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Stanford University (Psychology dept.—FMSF involvement): FMSF materials

Stephens, Inc.: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Stoneham Massachusetts Schools (high-school counseling CAN and FMSF ties): ICEP materials

Streamlight, Inc. (King of Prussia, PA): Jim Hougan, *Spooks*

Student Services, Framingham State College (CAN and FMSF ties): ICEP materials

Sullivan & Cromwell (legal firm repeatedly involved in CIA interests): John Prados, *President's Secret Wars*

Summit Aviation (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Sun Microsystem Federal, Inc. (Supplier): James M. Atkinson, Granite Island Group

Survey Research Center (SRC), University of Michigan (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

Swiss American Bank: Sen. John Kerry, Sen. Hank Brown, The BCCI Affair: *A Report to the Committee on Foreign Relations*

Symbionese Liberation Army (SLA—MK Ultra spin off)

Syracuse Research Corporation (Supplier): James M. Atkinson, Granite Island Group

Systematics, Inc. (Clipper chipp and PROMIS): Ralph McGehee, *CIA Namebase*

Systems Consultants, Inc. (mind control related): Alex Constantine, *Psychic Dictatorship in the USA*

Systems Services International: David Corn, *The Blond Ghost*

Task Force on Missionaries and Cults, Jewish Community Relations Council of New York (CAN and FMSF ties): ICEP materials

Temple Emmanuel (Beverly Hills—CAN and FMSF ties): ICEP materials

TGS International Limited : Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

The Aquatic Club: Jonathan Kwitney, *The Crimes Of Patriots*

The Aviary: Ralph McGehee, *CIA Namebase*

The Bourbon and Beefsteak Bar and Restaurant (CIA spying on US military on R&R): Jonathan Kwitney, *The Crimes Of Patriots*

The Broyhill Building (Arlington—houses CIA training facility): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

The Cult Observer (publication of AFF): AFF materials—see also ICEP

The Law Association for Asia and the Western Pacific: Jonathan Kwitney, *The Crimes of Patriots*

The New Republic (periodical, disinformation source): David Corn, *The Blond Ghost*

The Public Interest (academic journal): *Alex Constantine, Psychic Dictatorship in the USA*

The Riverside Lodge of the Ordo Templis Orientis (A.K.A. The Solar Lodge of the OTO—MK Ultra spin off)

The Second National Bank of Homestead (Florida—drug money laundering): Jonathan Kwitney, *The Crimes Of Patriots*

The Texas Tavern (CIA spying on US military on R&R): Jonathan Kwitney, *The Crimes Of Patriots*

The Washington Monthly (ex-intelligence agent and columnist Christopher Pyle writes article exposing military intelligence blunders in an area CIA wishes to have more control): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

The World Finance Corporation (the largest narcotics investigation of the decade (70's) against this firm was dropped at CIA request): Jonathan Kwitney, *The Crimes Of Patriots*

Time Magazine (knowingly hired CIA operatives as reporters, edited/killed stories at CIA direction, obtained/printed intelligence information after White House denied access): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Tractron (Vienna, Va.): Jim Hougan, *Spooks*

Trade Winds Motel (part of NIA, and sharing the same name as Operation Trade Winds, a project involving Robert Peloquin an Robert Vesco interests), Jim Hougan, *Spooks*

Trans World Oil: David Corn, *The Blond Ghost*

Trident Bank (Vesco operation): Jim Hougan, *Spooks*

TRW (Supplier): James M. Atkinson, Granite Island Group

UCLA School of Medicine (Psychiatry dept.—FMSF involvement): FMSF materials

UCLA School of Medicine, Psychiatry and Biobehavioral Sciences: Daniel Brandt, *Namebase Newsline*

Udall Corp. (Oliver North Iran-Contra): John Prados, *President's Secret Wars*

Union Bank of Switzerland : Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

United Fruit Company (the whole reason for the war in Guatemala, and steeped in CIA activities, including leadership by John Foster Dulles, former OSS): John Prados, *President's Secret Wars*

United Technologies (Supplier): James M. Atkinson, Granite Island Group

University of California (Psychology/English depts.—FMSF involvement): FMSF materials

University of California Medical School (Psychiatry dept.—FMSF involvement): FMSF materials

University of California, Berkeley (MK Ultra and significant Jonestown massacre ties through Dr. Lawrence Laird Layton, considered a cofounder of Jonestown)

University of Indiana, College of Foreign Affairs

University of Kansas (Psychology dept.—FMSF involvement): FMSF materials

University of Maryland (CAN and FMSF ties): ICEP materials

University of Miami, Zenith Technical Services: David Corn, *The Blond Ghost*

University of Michigan, Institute for Social Research (Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

University of Michigan, Survey Research Center (SRC—Intelligence funded PSYOPS projects): Christopher Simpson, *Science of Coercion*

University of Oklahoma (MK Ultra): Daniel Brandt, *Namebase Newsline*

University of Pennsylvania (Psychiatry/Social Work depts.—FMSF involvement): FMSF materials

University of Pennsylvania NOTE: There are many participants in CAN/FMSF/ICEP involvements not reflected by these comparatively few U of P listings

University of Pennsylvania, Experimental Psychiatry Laboratory (SEI involvement as well)

University of Pennsylvania, Graduate School of Education (CAN and FMSF ties): ICEP materials

University of Pennsylvania, Institute of Pennsylvania Hospital (Psychology/Psychiatric depts.—FMSF involvement): FMSF materials

University of Pennsylvania, Newman Center (CAN and FMSF ties): ICEP materials

University of Pennsylvania, Psychology in Education Division (CAN and FMSF ties): ICEP materials

University of South Carolina (mind control experiments in Voodoo): Alex Constantine, *Psychic Dictatorship in the USA*

University of South Carolina (see SEI)

University of Utah (MK Ultra)

University of Washington (Law and Psychology depts.—FMSF involvement): FMSF materials

University of Washington (FMSF ties)

University of Western Ontario (Psychiatry dept.—FMSF involvement): FMSF materials

University of Wisconsin (Psychology dept.—FMSF involvement): FMSF materials

USIA (United States Information Agency): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

USIA Weapon Sales (a former local Portland area gun store): Harry Sweeney, *Fatal Rebirth*

Vanguard Service Corporation: Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Vector, Ltd. (Vesco operation): Jim Hougan, *Spooks*

Venture Fund (Vesco operation): Jim Hougan, *Spooks*

Vision Banc Savings: Jack Colhoun, "The Family That Preys Together," *Covert Action Quarterly*

Wackenhut: Jim Hougan: Jim Hougan, *Spooks*; Michael Riconosciuto, Wackenhut/CIA operative

Wallach Associates, Inc. (Intelligence executive placement agency): John Pike, *American Federation of Scientists*

Wandel and Goltermann (Supplier): James M. Atkinson, Granite Island Group

Washington Post (CIA disinformation source): Victor Marchetti/John D. Marks, *The CIA and the Cult of Intelligence*

Wayne State University Law School (Law and Psychiatry depts.—FMSF involvement): FMSF materials

Western International Ground Maintenance Organization (WIGMO): John Prados, *President's Secret Wars*

Westinghouse (Supplier): James M. Atkinson, Granite Island Group

Westmont College (Santa Barbara—CAN and FMSF ties): ICEP materials

Weston High School (city not specified, presumed NY, high-school counseling CAN and FMSF ties): ICEP materials

William Cook and Co.: John Marks, MK Ultra Behavior Control Experiments Document Collection

World Marine, Inc. (Douglas Schlachter and Opal document related): Jonathan Kwitney, *The Crimes Of Patriots*

Yale University (Psychology dept.—FMSF involvement): FMSF materials

Young People and Cults (publication of AFF): AFF materials—see also ICEP

Zapato Off-Shore Oil Company (George Bush front, Houston, 1963): Mark Lane, *Plausible Denial*

Zapato Petroleum Corp. (George Bush front, Houston,1963): Mark Lane, *Plausible Denial*

Zenith Technical Enterprises (Bay of Pigs command central operating on the University of Miami campus): John Prados, *President's Secret Wars*

APPENDIX III

More about Bugs

The following was provided by James M. Atkinson. If you can believe it, it this is merely an edited version of a much larger volume of Internet material available on the topic of TSC/TSCM (Technical Security Counterintelligence or Countermeasures). See the contact info at the end of this section if you wish to get a full and current version of the list. The intent here is to show the complexity and vastness of the topic and to illustrate why, if you think you have a bugging problem, you need to call in a TSCM professional.

Mr. Atkinson starts with a warning to be wary of fraudulent TSCM types who "try to convince you that bugs don't operate above 1 GHz or 3 GHz" or who approach you with "classified government bug detection equipment." The former is usually a sign you are dealing with an underequipped amateur who cannot afford the gear needed to cover the full spectrum of a potential threat. The latter is usually a fraud, someone who will offer a $350 RF field detector (which can detect some kinds of bugs) for thousands.

Atkinson cites a corporate officer who complained his $70,000 "classified" detector, just purchased, did not work, only to find out it was worth $395 off the shelf and in working order.

Also, a lot of private-eye and TSCM schools mislead students into thinking a few thousand dollars is all they need to provide full service, typically based on such limited technology. This trickles down to the consumer and can result in undetected threats and a false sense of security. According to Atkinson, "These schools and spy shops are trying to modify reality and the laws of physics to help them pad their bank accounts. A legit TSCM inspection (even a basic one) requires at least $250,000 worth of equipment."

Here is Atkinson's summary of devices used for TSCM operations. Some of the information may be far more technical than the casual reader has use for—don't worry about trying to memorize or even fully comprehend every bit of it. The point here is to increase your awareness of the technological sophistication available to your opponents and the sophistication which will likely be required to detect, with any assurance, that you have no genuine current surveillance threat or have found all threats that may exist. Having the information here will also aid you in determining how good your TSCM service provider is. Ask him to review his findings in each of the frequency ranges, technologies, and conditions as outlined here—and compare his answers and comments with some of the limits/specs as shown:

> Expect to see less than 0.1-10 mW maximum (very low output wattage or signal strength) at the transmitting antenna—do not expect the signal to be present for more than 20 µs to 100 µs. The device may use AC power circuits, telephone wiring, or HVAC systems as the transmission path (3 kHz to 300 MHz and up), and may also use spread-spectrum technology. Every cubic centimeter of the facility must be inspected.
>
> Remember, bugs are often installed in groups of at least three: the one that's easy to find (the fool's bug), the one that you'll find if you really work hard (the pro bug), and the one that's almost impossible to find (the spy's bug). The only thing on earth that can find a bug is a pair of well-trained eyes and a set of callused and experienced hands. The test equipment only suggests to the inspector where to look. There are no magical black boxes that find bugs.

Simply everything, from phone rooms and riser closets to your boots, must be checked for tampering and electromagnetic anomalies (such as RF activity). All electrical outlets, light fixtures and switches, circuit breakers, distribution boxes, electric meters, and transformers must be checked for tampering and electromagnetic anomalies. The transformer is the most important of these, as it is commonly used to facilitate technical surveillance.

The microphone and cameras can be hundreds of feet away from the transmitter or recorder (be sure to check all potential transmission paths). Use a digital spectrum analyzer and a wide-band receiver. maximum dispersions of 100/200/500 kHz are ideal. If a given bug signal is "scrambled," it is likely nothing more than simple voice inversion; a circuit to "de-scramble" it costs around $20.

Author's note: The next paragraph describes a key element of a good TSCM survey. It is saying that you check to see what RF is being broadcast from the target site over time and space before you even conduct a site search for devices. Find when and where the signals output and in what direction—finding the listening post would be a good thing, too. This is concluded with a longer and more detailed list of frequency information. Don't be tempted to scan this information superficially—there is some real eye-opening stuff if you actually READ THE WORDS and take your time. This is an encapsulated description of your opponent's potential and may give you clues as to the scope of your problem—who your enemy really is, perhaps, since some of this stuff is used by specific groups or has exotic origins.

RF Spectrum Analysis and monitoring should take place for at least twelve solid hours before a regular sweep (72 hours or more is preferred). This part of the inspection is performed the day before the actual sweep and involves monitoring the ambient electromagnetic spectrum at locations AWAY from the actual facility (distances range from several yards to several miles, and spiral search patterns are normally used).

Most professional RF bugs will generally have a transmit frequency between 3 kHz and 9 GHz. However, low-cost, high-performance bugs that oper-

ate on frequencies between 3 kHz and 21 GHz are readily available. For someone willing to spend a little more money, bugs can be easily obtained which operate in the 30 to 50 GHz range. This means the person performing a TSCM inspection must always inspect well above and below these frequencies.

The radio frequency and signal analysis portion of the TSCM inspection must cover at least 3 kHz to 60 GHz (220 GHz is ideal).

Audio Detection 20 Hz–30 kHz Base Band Audio
Ultrasonic Detection 10–150 kHz Ultrasonic Audio
VLF Detection-Audio 300 Hz–100 kHz Video Cameras & Tape Recorders
VLF Detection-RF 3–500 kHz Video Cameras & Tape Recorders
VLF Detection-Audio 300 Hz–150 kHz Microphone/Ultrasonic Chirping
Carrier Current Bugs 300 Hz–50 MHz 99% Voice (CC and PLA)
Carrier Current Bugs 10–350 MHz 99% Voice (AC Mains Antenna)
RF Bugs-HF 3 kHz–50 MHz 99% Voice
RF Bugs-VHF 30–300 MHz 10% Video/80% Voice/10% Data
RF Bugs-UHF 300–900 MHz 25% Video/60% Voice/15% Data
RF Bugs-Microwave1 3 GHz–900 MHz50% Video/40% Voice/10% Data
RF Bugs-Microwave2 3–18.5 GHz 65% Video/10% Voice/25% Data
RF Bugs-Microwave3 18.5–40 GHz 70% Video/25% Voice/10% Data
RF Bugs-Microwave4 40–325 GHz Mostly Data and Audio Bugs

UV/infrared:

150–450 nm	Modulated UV Light Bugs
350–700 nm	Modulated Visible Light Bugs (450–675 nm very common)
700–1100 nm	Audio Transmitters/Lasers (880–950 nm very common)
800–1510 nm	Audio Transmitters/Laser Microphones (rare)
750–900 nm	Night Vision Illuminators
850–1750 nm	IR Bugs and IR Illuminators

Optical bugs installed INSIDE light bulbs and fixtures:

450 nm	Modulated Tungsten Bugs
490 nm	Modulated Sodium Bugs
575 nm	Modulated Fluorescent Bugs

Note: Most military, intelligence, and diplomatic TSCM inspections look for devices between 3 kHz to 350 MHz for Carrier

Current/PLA, 20 kHz to 40 GHz for regular RF radio devices, and directional microwave devices from 0.3 to 220 GHz+.

High-threat frequency bands:

50–750 kHz	Carrier Current Bugs (power lines or phone lines)
25–80 MHz	Ultra Low Power Bugs (microwatt devices)
65–130 MHz	Micro power Part 15 devices (FM broadcast band)
135–150 MHz	Body Wires and Wireless Microphones—Band I
150–174 MHz	Body Wires and Wireless Microphones—Band II
174–225 MHz	Body Wires and Wireless Microphones—Band III
295–310 MHz	Spread-Spectrum and Micropowered Bugs (microwatt devices)
350–430 MHz	Audio/Video Bugs (microwatt and spread-spectrum devices)
430–550 MHz	Audio/Video Bugs (434 MHz popular)
890–960 MHz	Audio/Video Bugs (902–950 MHz popular)
1.1–1.93 GHz	Video and Audio
2.4–2.55 GHz	Video and Audio (Extremely Popular)
6.2–7.5 GHz	Video and Audio
8.1–13 GHz	Video and Audio (Extremely Popular)

Bugging devices operating below 22 GHz are very inexpensive and easy to buy. Devices operating between 22 to 60 GHz are more expensive but just as easy to secure. Devices operating on frequencies above 60 GHz tend to be expensive and can be very difficult to obtain.

3 kHz	Typical Audio Band
3–700 kHz	Skin Effect (Non-Radiating)
700 kHz–3 MHz	Non Radiating, Conducted RF
3–300 MHz	Conducted RF, Free Space Radiating
300 MHz–3 GHz	Free Space Radiating RF, Slightly Directional
3–22 GHz	Free Space, Low Attenuation, Highly Directional
22–60 GHz	Water-Vapor Absorption Band
60 Ghz–3 THz	Limited Usage For Covert Surveillance

Note: frequencies between DC and 22 GHz are used for covert eavesdropping, Major realistic threat up to 60 GHz. The 70 to 110 GHz M-band is also becoming very popular due to new technology which has drastically reduced attenuation in those frequencies.

Common wireless bugs (low power—well under 35 to 50 mW):

44.5–51 MHz	Baby and Room Monitors (49.83, 49.845, 49.875 kHz, etc...)
72.1–75.4 MHz	Hearing Assistance Systems

54–150 MHz	Kit Bugs
98–108 MHz	FM Bugs
112–142 MHz	FM Bugs
140–160 MHz	FM Bugs
60–320 MHz	Low Cost Kit Bugs
398–406 MHz	DECO Bugs (398.6/605, 399.45/455, 399.025/03, 406 MHz)
25–450 MHz	European/English Kit Bugs
150–216 MHz	Typical VHF "Body Wire" & Pro-Grade Bugs
109–140 MHz	Digital VHF Pro-Grade Bugs
138–174 MHz	Typical "Spy Shop" & LE Cheap VHF Bugs (155–172 MHz popular)
140–150 MHz	Popular Xandi Flea Powder Kits (143/144 MHz)
150–170 MHz	Popular Japanese Flea Powder Kits (under 5 mW)
150–220 MHz	47 CFR 2.106 (NG115) Authorization
395–410 MHz	German UHF Bugs (PK Electronics)
365–455 MHz	English UHF Bugs (Lorraine/Ruby Electronics)
219–530 MHz	English UHF Wireless Microphones (300-500 popular)
470–608 MHz	Commercial Wireless Microphones
730–806 MHz	Commercial Wireless Microphones
310–980 MHz	Sony Bugs (0.1–3 mW, spread-spectrum)
470–489 MHz	Sony Bugs (2.5–20 mW, WFM, ultra low power)
770–810 MHz	Sony Bugs (2.5–20 mW, WFM, ultra low power)
902–928 MHz	Sony Bugs (2.5–20 mW, WFM, ultra low power)
947–954 MHz	Sony Bugs (2.5–20 mW, WFM, ultra low power)
889–960 MHz	Modified Cordless Phones (S/S & hoppers)
380–480 MHz	Video Bugs—US
430–900 MHz	Popular US Video/Audio Bugging System
890–960 MHz	Video Bugs—US (902–928 MHz Hot)
905–928 MHz	Video/Audio Consumer Products (i.e. Recoton)
1.1–1.4 GHz	Video Bugs *Very Hot in U.S., England, France, etc.*
1.7–1.93 GHz	Video Bugs—US
2.4–2.5 GHz	Video Bugs—US *** VERY Popular ***
3.5–4.5 GHz	Video Bugs *very popular in European countries*
5.725–5.85 GHz	Video Bugs—US *** VERY Popular ***
6.2–7.5 GHz	Video Bugs—US *** VERY Popular ***
8–12 GHz	X-band Audio/Video Bugs (Extremely Popular w/ Government)
20–26 GHz	K-band Audio/Video Bugs (Popular w/ Government)
70–110 GHz	M-band Audio/Video Bugs (Gaining Popularity)

Subcarrier detection:

10–500 kHz	Most Commonly Used Subcarrier Bugging Frequencies
15–150 kHz	Typical Broadcast FM/TV Subcarriers (TV/FMSubC)

0–15 kHz	Typical Broadcast FM L-R Signal (mono)
19 kHz	Typical Broadcast FM Subcarrier—Pilot
23–53 kHz	Typical Broadcast FM Subcarrier L-R Signal (stereo, 38 kHz center)
57 kHz	Typical Broadcast FM Subcarrier—RBDS/EAS
67 kHz	Typical Broadcast FM Subcarrier SCA/Musicast/Muzak
92 kHz	Typical Broadcast FM Subcarrier SCA/Musicast/Muzak
15–105 kHz	Typical Broadcast Television Subcarriers (TVSubC)
0–15 kHz	Typical Broadcast TV Audio L-R Signal (Mono)
15.75 kHz	Typical Broadcast TV Subcarrier–Pilot
31.5 kHz	Typical Broadcast TV Subcarrier L-R Signal (Stereo)
62.94 kHz	Typical Broadcast TV Subcarrier—SAP Secondary Audio
102.27 kHz	Typical Broadcast TV Subcarrier—Cue Channel
2–10 MHz	Typical Video Component Subcarriers (4.2–8 MHz common)
5–750 kHz	Viable Subcarrier Threat (Audio)
5 kHz–15 MHz	Viable Subcarrier Threat (Video)

Note: A typical FM broadcast can easily contain 2 to 12+ subcarrier voice channels in addition to the main signal, and subcarriers can have their own subcarriers.

"Tactical" bugs:

225–400 MHz	"Throw away" bugs (10 µW–300 mW "beer can" bugs)
290–330 MHz	Micro-powered Bugs (5 µW–10 mW "cigarette butt" bugs)
180–430 MHz	Spread-Spectrum Wafer Bugs (1.5 mm × 10 mm × 2.9 mm)
30–500 MHz	Tactical Repeaters (75 mW–300 mW)
285–400 MHz	Tactical Repeaters (50 mW–10W)
100–152 MHz	VHF Tactical Repeaters (300 mW–25W)
135–174 MHz	VHF Tactical Repeaters (300 mW–25W)

VLF and carrier-current bugs:

9 kHz—490 kHz	Carrier Current 47 CFR 15.219 Auth (250 mV max.)
490 kHz–1.705 MHz	Lossy Cable 47 CFR 15.221 Auth (1000 mV max.)
450 kHz–30 MHz	PLA Systems 47 CFR 15.207 Auth (30 mV @ 1 ft/30 ft max.)
3–200 kHz, 300 mW	High Grade Pro Bugs (over $500 each)
100–200 kHz, 50–100 mW	Older Bugs
120–200 kHz, 30–50 mW	Pre-1990 intercoms
200–300 kHz, 30–50 mW	Post-1990 intercoms
300–400 kHz, 250–450 mW	TELCO Line transmitters (355 kHz popular)
300 Hz–30 kHz	Cable TV Carrier—Hard-wired Microphones (base-band audio)
30–300 kHz	Cable TV Carrier—Coaxial Bugs (wide-band audio/video)

100–450 kHz	Threat Window #1 Most CC Bugs
3 kHz–3 MHz	Threat Window #2 Expensive "Pro Grade" Bugs
5 kHz–32 MHz	Threat Window #3 Popular WJ Carrier Current Rcvr
3 kHz–50 MHz	Threat Window #4 Realistic Threat Window for Telephone Wire
15 MHz–70 MHz	Threat Window #5 Audio/Video "Micro Wire" RF circuits

VLF devices:

25 kHz—0 kHz	Tape Recorder Bias Osc-Low End (35–45 kHz common)
80 kHz—145 kHz	Tape Recorder Bias Osc-Mid Range (88.2, 96, 100 kHz common)
100–325 kHz	Tape Recorder Bias Osc-Pro Grade (100, 150, 300 kHz common)
40–50 kHz	Tape Recorder DAT/Hi8 (44.1/48 kHz common)
4–35 kHz	Recorder Audio Servo Noise (10–20 kHz common)
7–35 kHz	Video Camera VLF Detectable emissions
15.75 MHz	Common NTSC Video Camera
15.734 MHz	CCD/PCB Video Camera (very easy to detect)
15.625 MHz	Common Video Camera

Note: Be aware of ultrasonic/audio emisions from most VLF devices. (Use a EOD/Bomb Tech Stethoscope, and/or Ultrasonic Spectrum Analyzer.)

25–50 MHz	"Bumper Beepers" (38–47 MHz very popular)
135–170 MHz	"Bumper Beepers" (150–170 MHz very popular)
450–512 MHz	"Bumper Beepers"
903–912 MHz	"Bumper Beepers"
918–927 MHz	"Bumper Beepers"

Note: British-made LYNX video bugs and cameras are frequently built into old bricks, wooden joists, logs, gate posts and such... VERY dangerous asset and easily concealed. French-made DGR spread-spectrum video cameras are hidden inside functional electrical outlets, system supports up to 240 cameras on same circuit, video and audio conducted over power lines. Commonly used for hotel-room buggings.

136–150 MHz	Wireless microphone/Body Wires (Special Order)
150–174 MHz	Wireless microphone/Body Wires (Standard)
170–220 MHz	Wireless microphone/Body Wires (Special Order)
200–470 MHz	Wireless microphone/Body Wires (Special Order)
470–608 MHz	Wireless microphone/Body Wires (70 mW max)
945–955 MHz	Wireless microphone/Body Wires (VR series)
130–240 MHz	MicroEar—In-ear FM-NB rcvr system

138–190 MHz	MicroEar—In-ear FM-NB rcvr system
190–220 MHz	MicroEar—In-ear FM-NB rcvr system

X10/BSR—home AC-control systems available in many department and specialty stores can be used by the pro as the basis of a bug network within a home or other site:

290–305 MHz	Transmits RF over AC power lines—Audio (301-303 hot)
301–315.5 MHz	Transmits RF over AC power lines—Audio (310/312 hot)
410–426 MHz	Transmits RF over AC power lines—Audio (418 hot)

Radio Shack products of note:

120–200 kHz	FM Wireless Intercom Systems (uses AC mains)—Older Units
200–270 kHz	FM Wireless Intercom Systems (uses AC mains)
300–400 kHz	FM Wireless Intercom Systems (uses phone wires, 355 popular)
35–50 MHz	FM Microphones (49.830, 49.855, 49.890, 37.600 Popular)
75–110 MHz	Lavalier Microphones (FM Broadcast Band)
50–290 MHz	FM Microphones (CM-421, below 5–50 mW)
160–230 MHz	FM Mics (169-176 MHz popular, 5–50 mW max, 15 mW typical)
700–950 nm	Infrared Audio Transmitter (150 kHz carrier typical)
173.075 MHz	LOJACK Auto tracking system beacon (200ms burst every second). The LOJACK Corporation autotracking beacon system can be remotely activated via FM subcarrier and be used on vehicles.

Police speed enforcement radar:

10.450–10.6 GHz	X-Band
11.488–11.628 GHz	RD Detector
22.976–23.256 GHz	RD Detector-2nd Harmonic
24.05–24.25 GHz	K-Band
33.4–36 GHz	Ka-Band
700–1100 nm	Laser Threat

Electronic article surveillance and anti-shoplifting systems:

8.1–9.3 MHz	Checkpoint (Hi-Q Tags) 8.2 MHz Common
57.75–58.75 kHz	Sensormatic (Magnetic) Books, CDs, and Tapes
915, 1830 MHz	Knogo Microwave Resonant Adhesive Labels (the anti-theft tags that set off sensors at the doors of department stores)

Metal detectors:

5–210 kHz	Walk Through and Hand-held Units (i.e. Garrett)

WARNING: The area between 600 MHz and 9 GHz is EXTREMELY DANGEROUS as an enemy asset, as the eavesdropping equipment in that range is inexpensive, very low power, and highly directional. Additionally, most TSCM people tend not to check frequencies above 1 or 3 GHz (because the necessary equipment is too expensive for them to buy).

Surveillance satellite frequencies (note: mostly wide-band spread-spectrum/LPI channels):

220–450 MHz	
1.2–1.4 GHz	
1.7–1.9 GHz	(1.76–1.84 GHz active)
1.9–2.2 GHz	(2.115 GHz active)
4.9–5 GHz	
5.5–8.73 GHz	
10.6 -12.8 GHz	(11.7–12.2 GHz active)
17.8–22.5 GHz	(Low Orbit SIGINT/IMINT Birds)
23.6–24 GHz	(Low Orbit SIGINT/IMINT Birds)
25.5–25.7 GHz	(Low Orbit SIGINT/IMINT Birds)
22.8–33.5 GHz	(SIGINT Birds)
42.5–47 GHz	(High Orbit SIGINT/IMINT Birds)
50.3–52.4 GHz	(High Orbit SIGINT/IMINT Birds)
78–85.5 GHz	(High Orbit SIGINT/IMINT Birds)
86.3–98.3 GHz	(High Orbit SIGINT/IMINT Birds)

Note: 95–275 GHz is used for government surveillance applications and operations; however, the usage is fairly limited. Surveillance satellite can be anywhere between 200 MHz and 325 GHz, mostly spread-spectrum.

40.12 MHz	Federal Shared Mobile Locator Transmitters "Bumper Beepers" *HOT*

40.17 MHz	Federal Shared Mobile Locator Transmitters "Bumper Beepers" *HOT*
40.22 MHz	Federal Shared Mobile Locator Transmitters "Bumper Beepers" *HOT*
40.27 MHz	Federal Shared Mobile Locator Transmitters "Bumper Beepers" *HOT*
164.9125 MHz	FBI Surveillance
165.9125 MHz	ATF F5 Surveillance
166.2875 MHz	ATF
170.4125 MHz	ATF
172.2 MHz	DOJ/DEA CH.1
171.6 MHz	DOJ/DEA CH.2
406.275 MHz	Secret Service
407.8 MHz	Secret Service, CIA, State Department
408.05 MHz	Federal Shared
408.575 MHz	Federal Shared
409.4 MHz	Federal Shared
408.5 MHz	Secret Service
408.975 MHz	Secret Service
418.05 MHz	DEA Low Power
418.075 MHz	DEA Low Power
418.575 MHz	DEA Low Power
418.75 MHz	DEA
418.675 MHz	DEA
418.9 MHz	DEA F2 CINDY (416.325 MHz) Surveillance
418.75 MHz	DEA F3 GAIL Surveillance/Strike Force
418.675 MHz	DEA F4 EMILY (416.325) Surveillance
960–1215 MHz	Spread-Spectrum Systems (Wide-band)
8–13 GHz	Very popular wide-band, low power (under 10–100 mW) video/audio devices

Generally recognized federal bug/spy bands:

25–75 MHz	Primary
135–175 MHz	Primary
225–440 MHz	Primary
1.71–1.95 GHz	Primary
8.3–12.5 GHz	Primary
890 MHz–5.5 GHz	Secondary
7–13 GHz	Secondary
10–39.6 GHz	Secondary
0.902–0.928 GHz	Popular Commercial FH/DS Devices

1.71–1.755 GHz	DEA Audio/Video Bugs (over 1,400 bugs purchased in 1995)
1.71–1.755 GHz	DOJ Audio/Video Bugs (0.25–0.5W)*
1.71–1.85 GHz	Treasury Video Surveillance Systems
2.4–2.484 GHz	Popular Commercial FH/DS Devices
4.635–4.66 GHz	Treasury Video Surveillance Systems

Government microwave-based surveillance gear seems to be running between 900 MHz to 5 GHz, with a few systems operating on the 7/8 GHz bands. Keep in mind that the pros love to use ultra low-power devices, which use power lines as their transmission medium/antenna (9 kHz to 300 MHz). Devices typically operate below 10 mW, often below 1 mW. The devices typically use Wide FM and use voice inversion encryption...VERY easy to demodulate.

The Department of Justice (DOJ) just took delivery of a large number of video transmitter modules with operating frequencies between 8 GHz and 11 GHz (PLL field programmable), 10 mW RF output (max), nominal 8.5 mW, power draw below 35 mA, base-band video transmission, not spread spectrum. All modules have audio inputs (solder tab), standard audio subcarrier, audio section may be disabled to conserve power. Minimum effective range indicated as 2,700 feet line of sight, and 1,500 feet rural. Power requirements seem to correlate to 9 VDC lithium batteries. I would estimate the range to be below 500 feet with a unity gain antenna. A number of the units came reinstalled in fake squirrel and bird nests with a low light auto iris CCD camera (unknown manufacturer, possibly Kodak). I've seen similar units used by the DEA (installed under tree bark).

From what I can see on the physical specs, looks like the transmitter and camera combined are two-thirds the size of a standard 9 VDC battery. The government paid $874 per module (transmitter only). I wonder if these are the "tree frogs" that the boys at Quantico were trying to get bids on back in September? It's only a matter of months before these devices get "lost in the field" and reappear in the private sector.

Note: According to a recently obtained DOJ surveillance training manual, "The typical range for the 28 GHz devices is six miles, the typical range of the 2.4 GHz is 30 miles, and the typical range for the 1.7 GHz is 44 miles ... frequency-modulated applications should operate below 3 GHz to take advantage of the favorable frequency propagation characteristics of that part of the spectrum....

Frequency hopping, direct sequence, and spead spectrum devices should operate above 1.5 GHz; this will prevent the emissions from being detected by electronic countermeasures."

Also, Wide-Band Frequency Hopping centered on various UHF-TV channels (ie: 510 or 670 MHz with a hopping width of ±25 MHz.) Keep in mind that the federal government can use virtually any frequency between DC and light.

Spread-spectrum/hopping frequencies (legitimate industrial equipment very inexpensive, easy to buy and build):

9 kHz–54 MHz	Current Carrier Devices (very popular for video)
26.96–27.28 MHz	Popular Spread-Spectrum Devices
40.48–40.88 MHz	Popular Spread-Spectrum Devices
902–928 MHz	ISM band A (Very Popular)
2400–2484 MHz	ISM band B (Very Popular)
5725–5875 MHz	ISM band C
10500–10550 MHz	ISM band D
24000–24250 MHz	ISM band E

Spread-spectrum bands often used for eavesdropping (very inexpensive):

50–54 MHz @ 6m	Amateur Radio Equipment (STA)
144–148 MHz @ 2m	Amateur Radio Equipment (STA)
222–225 MHz @ 1.25m	Amateur Radio Equipment (STA)
420–450 MHz @ 70 cm	Amateur Radio Equipment (47 USC 97.305)
902–928 MHz @ 33 cm	Amateur Radio Equipment (47 USC 97.305)
1240–1300 MHz @ 23 cm	Amateur Radio Equipment (47 USC 97.305)
2300–2450 MHz @ 13 cm	Amateur Radio Equipment (47 USC 97.305)
3300–3500 MHz @ 9 cm	Amateur Radio Equipment (47 USC 97.305)
5650–5925 MHz @ 5 cm	Amateur Radio Equipment (47 USC 97.305)

Spread-spectrum bands occasionally used for eavesdropping:

10–10.50 GHz @ 3 cm	Amateur Radio Equipment (47 USC 97.305)
24–24.25 GHz @ 1.2 cm	Amateur Radio Equipment (47 USC 97.305)
47–47.2 GHz @ 6 mm	Amateur Radio Equipment (47 USC 97.305)

Spread-spectrum bands rarely used for eavesdropping (very expensive):

75.5–81 GHz 4.0 mm	Amateur Radio Equipment (47 USC 97.305)
119.98–120.02 GHz 2.5 mm	Amateur Radio Equipment (47 USC 97.305)
142–149 GHz 2.0 mm	Amateur Radio Equipment (47 USC 97.305)

241–250GHz 1.0 mm	Amateur Radio Equipment (47 USC 97.305)
300 GHz–Light (3 THz)	Amateur Radio Equipment (47 USC 97.305)

Note: Most common spread-spectrum/hopping equipment will hop at speeds between 100 and 50,000 hops per second. Equipment is readily available that hops even faster (100,000 to 300,000 hops per second). Dwell times can be as small as 1 µs (one widely used system uses a dwell time of 3–5 µs).

Out-band equipment:

ANY Television Broadcast or Cable TV Frequency
ANY FM radio Broadcast Frequency
ANY Paging or Beeper Frequency
ANY Cellular Telephone Frequency
820–960 MHz Modified (902-928) Cordless Telephones Modified
Amateur Radio Equipment (can be on ANY frequency)

Keep in mind that wide-band (non-ISM) spread-spectrum/hopping bugs are very difficult to detect (even if you are within a few feet).

All Spread-Spectrum devices are detectable but not without some difficulty. Once spread-spectrum/hopping bugs have been located (on the RF spectrum) all that can be done is to locate the source of the emission ... it is virtually impossible to demodulate a spread-spectrum signal unless you have access to the key.

Also, a 500 mW spread-spectrum device can easily have an effective range of over twenty miles. In 1994, I field tested a spread-spectrum LPD/LPI hand-held radio designed for downed pilots. The power would vary between one half milliwatt to one full watt based the quality of the duplex link. With power levels below 25 mW, we could communicate clearly at a distance of 45 miles on the open ocean (from a life raft) and 15 miles in the dense woods of Maine. When the device was tested in a dense urban area (as a bug), a range of 2,500 to 8,600 feet was obtained, wtih a power output below 15 mW.

Use search receivers with a wide-band infrared-frequency output (700 MHz), and a wide infrared bandwidth (over 7 to 70 MHz). Look for the signature wide-band hump and then detune the frequency of the signal to locate the device. Don't be suprised if you find a table leg, bulletin board, cube divider, clock, or wall emitting spread-spectrum RF energy.

All TSCM people know of products manufactured by Audio Intelligent Devices, Inc. (author's note: a CIA proprietary sold off to "private interests"), but few know the actual frequencies they use or what they look like. The devices are VERY popular with the law-enforcement crowd, private investigators, and corporate-security types and is greatly overpriced. It's also fairly easy to detect. AID bills itself as "The world's largest manufacturer of electronic intelligence equipment and specialized protective systems." AID was founded in 1970 and was sold in 1992 to Westinghouse. (Westinghouse is currently selling TONS of equipment to the DEA and the state department.)

AID bug frequencies:

135–150 MHz	Special Order/Secondary Band
150–174 MHz	Standard/Primary Band (most popular)
216–220 MHz	Special Order
400–470 MHz	UHF Repeaters
21–80 MHz	Very Low Power WFM (0.5 mW–10 mW) Special Order Only
36–39 MHz	Very Low Power WFM (0.5 mW–50 mW)
80 kHz–200 kHz	"Line Carrier" Microphone Systems
30 kHz–700 kHz	Spread-Spectrum Current Carrier Devices
1700–1900 MHz	25-250 mW Video and Audio Bugs (Mostly DEA/DOJ stuff)
2400–2484 MHz	25-250 mW Video and Audio Bugs

Note: AID devices are often re-tuned for out-band channels, so be careful. If the signal is "scrambled" it is nothing more than simple voice inversion, and a circuit to "de-scramble" costs around $20. 15 MHz to 500 MHz is the primary threat, 500 MHz to 3 GHz is the secondary threat, and a "line carrier" threat is from 30 kHz to 750 kHz.

If the person planting the bug suspects that a TSCM inspection may be conducted, AID suggests a frequency between 30 MHz to 50 MHz, sensitivity of the receiver should be better than 0.18 μV/–122 dBm. The mode is usually wide-band FM. Also, keep in mind that AID devices are frequently used for illegal buggings, so be familiar with their realistic specs, expect power outputs well under 50 mW, and expect to see the AC power circuits being used as the antenna. Note: Mike Langley at the National Intelligence Acadamy (NIA), a CIA operation, reports that AID/NIA/Westinghouse is no longer providing TSCM training and stopped producing TSCM products in 1997.

HDS—Household Data Services:

50–750 kHz	Carrier Current Audio System
120–400 kHz	Carrier Current Audio System
138–174 MHz	Wireless microphone/Body Wires (8KR Series 0.1–30 mW)
150–174 MHz	Wireless microphone/Body Wires (ATX Series 0.1–30 mW)
174–230 MHz	Wireless microphone/Body Wires
350–440 MHz	Audio/Video Transmitters
470–608 MHz	Audio/Video Transmitters
570–928 MHz	Audio/Video Transmitters (Spread-Spectrum Popular)
1,000–1,500 MHz	Low Power Audio/Video Transmitter (10–100 mW max)
1,425–1,450 MHz	Low Power Audio/Video Transmitter (10–100 mW max)
1,700–2,700 MHz	Audio/Video Transmitters 2.4-2.5 hot (10–100 mW max)
1,710–1,900 MHz	Audio/Video Transmitters (10–100 mW max)
6,425–7,125 MHz	Low Power Audio/Video Transmitter (10–100 mW max)
8,100–8,700 MHz	Audio/Video Transmitter, 8.2/8.5 poplar (10–100 mW max)
10,200–10,700 MHz	Audio/Video Transmitter, 10.5 popular (10–100 mW max)
17,700–19,700 MHz	Low Power Audio/Video Transmitter (10–100 mW max)
20,000–24,600 MHz	Low Power Audio/Video Transmitter (10–100 mW max)

Sony—Wireless Microphones and Body Wires:

470–489 MHz	2.5–20 mW, WFM (110 kHz), Ultra low power
770–782 MHz	2.5–10 mW, Ultra low power—Chnl 64
782–794 MHz	2.5–10 mW, Ultra low power—Chnl 66
794–806 MHz	2.5–10 mW, Ultra low power—Chnl 68
770–810 MHz	2.5–20 mW, WFM (110 kHz), Ultra low power
902–928 MHz	2.5–20 mW, WFM (110 kHz), Ultra low power
947–954 MHz	2.5–20 mW, WFM (110 kHz), Ultra low power
960–970 MHz	2.5–10 mW, WFM (300 kHz), Audio Transmitter

Note: These low power devices have an adjustable frequency deviation that can be adjusted to as high as ±225 kHz and use a matched receiver. The system sells for under $2,500. Imagine a 3

mW transmitter operating at 782 MHz (snuggled up to the audio of the local TV transmitter) using a 100 kHz cue channel subcarrier. It has a life expectancy of at least 350 hours (using lithium cells) and a range of 1,500 feet indoors.

BMS:

BMS manufactures a line of pro-grade products used primarily for the Broadcast and Television markets, but their products are cheap and very small. Most of their voice/video/telemetry products (such as the BMT25-S) operate from 900 MHz–4 GHz (10 mW and 100 mW). The major threat is from the X-Band, and Ku-Band devices that operate at up to 13.5 GHz. Keep in mind the devices are as small as 1″ × 1″ × 3.3″ and can be run from a 12 VDC battery for days, if not weeks. Most of the devices use a variable frequency audio dual subcarrier between 4 to 9 MHz. They sell antennas, as well.

Microwave Surveillance System by AST:

Stock devices:

1.2–2.2 GHz
3.7–4.2 GHz
5.9–6.45 GHz

Special order devices:

1.2–2.8 GHz	The DOJ just bought a bunch of these
2.2–3.8 GHz	
3.2–4.8 GHz	State Department item
4.2–5.8 GHz	
5.2–6.8 GHz	Tech material mentions product available to law enforcement
8.5/8.8 GHz	

All functions are software-controlled, direct-sequence output, with a 60 MHz window for spread-spectrum. Author's note: These are sophisticated devices, a serious threat applied by serious players in serious circumstances. My understanding is that these transmit rotationally through multiple frequencies to make detection difficult. They can be programmed to repeat a given sequence in pairs of modulated frequencies which are demodulated on receipt—so you have to find the right pairs of frequencies (from up to 256 combinations) as well as the sequence to get close to "seeing" these things electronically. They can be also buried in the

phone system (PBX) in a way that allows many lines to be simultaneously tapped and transmitted. The box I examined measured 1" x 3.5" x 3" and took power from 8 to 16 VDC. Output power was fixed at 100 mW.

Delft Industries

I recently examined a device from Delft that was very similar to the X-Band units, except that the frequencies were higher and modulations were much more subtle. Small PCB was cemented into the rear of the unit, underneath the regular PCB (black rubber covered 1.5 cm * 4 cm * 0.8 cm). The unit consisted of two microphones, compander (compressor/expander) circuits, a power supply/regulator, and a modulator circuit. The compander circuit operated dual circuits around 120 Hz to 150 kHz.

There were no external modifications to the case, only very small variations in the power drain, no internal battery, several large surface mount caps. The entire unit was covered in double-sided surface-mount PCB, with digital, and analog, and RF circuitry. The only modifications to the alarm PCB was the cutting of several traces on the back of the PCB (near the emitter circuit). The Doppler alarm operated between 24 GHz and 24.25 GHz, intelligence seems to be a 480 KB digital datastream using the alarm signal as the carrier.

It looks as if one version of the product will also allow someone to deactivate a specific sensor remotely. According to the factory, the units are being shipped into Canada and Mexico in quantity and then transported into the U.S. in small numbers.

Texas Instruments:

I've heard from several engineers at TI that an unidentified government law-enforcement agency has them working on a super-compact thermal imaging system and video transmitter for covert surveillance. The system uses an electronic LCD chopper instead of the regular mechanical chopper. The devices, which contain microwave transmitters, are used for conducting long-term thermal surveillance.

Radio Shack:

Just finished playing with a nasty little Radio Shack (CM-421) single-channel VHF lavaliere microphone. While the product is designed for use in the 160 to 220 MHz range, it is designed to be recrystallized. The product can be easily retuned from 90 to 300

MHz (by the book), power output is variable via a pot from 5 mW to 50 mW. Current drain is around 40 mA at 50 mW and much lower for 5 mW output. Product is extremely stable, with adjustable deviations (to ± 100 kHz). Radio Shack will sell the transmitter alone for around $50 (I bought several to evaluate).

Corning Glass Fiber-Optic Devices:

I recently had access to some of the new fiber-optic devices out there and wanted to post some of the techniques by which they can be detected. These consist of three components and are manufactured by E-systems in Dallas, TX (a Department of Defense contractor). The entire installation kit fits into two briefcases.

1. "Front-End Microphone" is a small glass cylinder roughly 2.5 mm wide × 5 mm long, with a small 1.5 mm long pinhole tube on one end and a 3 to 12 ft. 50/125 fiber tail on the other. This part of the system is designed to be installed "pinhole" style. Pigtail cable is routed to and spliced into a "runner cable". The microphone contains small barbs to keep it in position with out the use of adhesives. A small 2.5 mm needle drill bit is used to drill the hole.
2. The "runner cable" is a 50 µm/125 µm fiber-optic bundle, typically 3 to 8 fibers are combined to allow a single runner to support 6-8 devices. This cable is flat and measures roughly 125 µm high and 0.75 to 1 mm wide. Cable has a minimum bend radius of 4 cm and is field terminated with a small, automated fusion splicer to the front-end microphone. This cable can be left loose or secured with an adhesive. Installation kit contains a small, flexible installation tube for carpet or wood panelling.
3. The "repeater" consists of a disguised box roughly 15 cm × 5 cm × 5 cm, with an optional battery pack/power supply/trickle charger (15 cm × 10 cm × 5 cm). The device can also be powered from AC mains. The repeater can be easily installed and hidden in a cinder block or within concrete on an outside wall. It looks like the device is for long-term installations.

The repeater uses up to eight fiber-optic outputs and an SMA connector for the base-band output. I suspect that this device can also be uploaded with transmission times. It also contains sufficient memory (32 MB) to hold four hours or more of compressed audio. It can also transmit (spread-spectrum) over phone or power lines

with a small adapter (I was not able to secure the frequencies, but I suspect somewhere between 200 kHz and 3 MHz).

Device appears to emit a RF digital signal using 64/128/256 QAM spread-spectrum modulation on programmable frequencies between 1.5 GHz and 8.5 GHz. Modulator is contained within a "flat pack" style antenna module. A 512 kbps base-band signal is supplied to the antenna (bitstream can go as high as 2 Mbps, the one I examined was set for 512 kbps).

Note: The repeater supplies the antenna with a base-band signal, control codes, and power. The modulator/transmitter is contained in the antenna. The device uses an RF guard channel that is used to deactivate all emissions (Go Mute) upon remote command.

This system uses a 50/125 Raw (a measurement of light-wave capacity for fiber optics) distribution system, the fiber is coated, but not jacketed or buffered in any way. The fiber has a frequency response between 1230 to 1550/1710 nanometers. I suspect it is standard single-mode (1500 nm) fiber strand. The repeater contains a low-power, single-mode, solid-state light source, a duplexer/splitter prism, and a light receiver. The light beam is transmitted into the fiber, travels to the front-end microphone, where it is reflected against an angled, vibrating membrane. The membrane causes a slight frequency shift in the light beam, which is reflected back to the repeater where it is picked off with a prism and solid-state detector.

Fiber-optic countermeasures:

There is no metal in the microphone or fiber-distribution system, and they CANNOT be detected by a Non-Lin test (a test which looks for nonlinear output). They cannot be detected with metal detectors, and no electromagnetic field is present on the front-end microphone.

The repeater section is fairly simple to detect with a Non-Lin unless it is installed within an exterior wall, which is often the case. The ideal way to detect one is to sweep the exterior of the building for RF emissions. Also, the unit tends to run VERY hot (at 110 to 135 degrees Fahrenheit) and should be visible as a thermal anomaly.

There is always a small amount of infrared leakage with these systems. The microphones can be detected with a infrared search at around 440 or 450 nm (you'll need a light source with at least

500,000 candle power, the Blue Light Ultra works well, or an Omnichrome). Once a suspect pinhole is found, it can be tested with a conventional spectrum analyzer with an infrared front end (Tektronix's SA-42 or SA-46 both work well).

Once the microphone is detected, it is a fairly simple matter to trace the line back to the repeater. Keep in mind that the system is designed to use three to eight microphones.

Here, Mr. Atkinson describes how to assemble a high-performance bug from standard components for under $100:

> Recently, I did some work designing an experimental, spread-spectrum wireless microphone. The goal was to see just how small and how cheaply a device such as this could be built. The device would need to have a range of at least 150 feet in a large building and be small enough to fit in a pocket. Furthermore, the device would have to run on standard batteries and cost less than $100 in materials.
>
> 1. I used two EPX-76 batteries, which gave up to three hours of usable audio, Configuring the device for use with a DL123A lithium battery increased the time to over four days.
> 2. The microphone consisted of two Siemens hearing-aid elements.
> 3. The spread-spectrum controller was a surface-mount WL-9010 from Wireless Logic.
> 4. I used a Mitsubishi codec (compression/decompression) with a noise-cancelling chip such as those commonly used in cellular telephones (this is why two microphones were necessary).
> 5. I incorporated a small potentiometer for output-power adjustment between 0.15 mW and 65 mW.
> 6. All components used were for surface-mount versions, hot-flow soldering was used for assembly
> 7. The entire circuit was assembled on a 0.3″ × 0.25″, double-sided, printed circuit board.
> 8. Range at 50 mW up to 260 feet.
> 9. The device was NOT detectable with an Avcom 65 until the antenna was within eight inches of the device.

All this confirms that spread-spectrum devices can be very small and cheaply made with readily available components.

If you would like to receive a much larger and more detailed list of information, with suggested strategies for TSCM procedures, send $35, plus $3 shipping and handling ($12 for overseas shipment). You should receive your frequency list in 2-4 weeks. If you would like to have a copy of the list faxed to you (as some countries will censor this page if sent through the mail), send $50, (plus $25 if overseas). You should receive your frequency list via fax in one week. Contact James M. Atkinson, Granite Island Group, 127 Eastern Avenue #291, Gloucester, MA 01931-8008; tel. (508) 546-3803; Web www.tscm.com.

Author's note: The Web site offers a great deal more good info and details on the topic than even the full list. This is the end of Mr. Atkinson's material.

APPENDIX IV

Supplemental Information on Caller ID and Crank Call Capture

It should be noted (again) that your enemy, especially if it's the government, will likely be using caller ID themselves. If you are being harassed by telephone calls, caller ID can aid in determining who your opponents are and, by working with the telephone company, seeking legal relief, where appropriate.

What this article does not cover is another kind of service offered by the telephone company that allows anyone who receives a crank or problem call to press a two-digit numeric code into their phone, which causes the telephone company computer to log the caller ID information of the offending party, even if call blocking is in place. To use this feature, you simply press *57 after BOTH parties hang up—something you can do at any time before the next inbound call is received at your end.

Use of *57 is not in and of itself a cure-all. The telephone company will not discuss the offending call. However, after several successive uses of the *57, a pattern of abuse will be exhibited. You may then contact the telephone company, who will evaluate this

pattern for any signs of a real abuse issue. If they have any reason to agree with you on the matter, there are several steps they may take on your behalf. These actions may vary depending on the local laws, telephone utility charter limitations, equipment capabilities, and the precise nature of the abuse.

Low-key actions can include warnings to the offending party, blocks to prevent any calls from that number from reaching you, or simply collection of additional evidence for possible legal action. The telephone company can put a recording system in place to capture calls from the offending party to gather this evidence. You could also record the conversation yourself, though, as mentioned earlier, it may be illegal.

A good strategy is to use Enhanced Caller ID which is, at least at first, configured to accept blocked calls. Use *57 to trap the offending calls, and work with the telephone company. If necessary, modify your Caller ID service to refuse blocked calls. Talk with your phone company service representatives to evaluate your need for the technology and the options it affords.

The following information on Caller ID comes from the October 1997 issue of the *FBI Law Enforcement Bulletin*, as obtained through Freematt Alerts on the Internet. (freematt@coil.com). The author, Mr. Williams, serves with the Electronic Surveillance Unit, Office of Investigations, at the U.S. Customs Service headquarters in Woodbridge, Virginia.

Caller ID: Maintaining Investigative Security

By David P. Williams

Investigators should take precautions in response to the growth of caller identification services.

The telephone has become such a staple of modern life that few people give it a second thought. When callers pick up the receiver, it is doubtful they consider the millions of signals being routed through switching stations that their call is about to join. They just know that when they want to check in with a family member across town or a business associate across an ocean, they only need to pick up the telephone. Even when power goes out in a community, the telephones generally continue to work. So, it might be easy to take this workhorse of the information age for granted.

However, advances in telephone service options—most notably caller identification services—require that law enforcement agencies take a close look at how they use the telephone. The growing

prevalence of caller identification services (generally referred to as caller ID) dictates that investigators take special precautions, especially during undercover operations.

Caller ID: Help or Hindrance?

As its name implies, the caller ID device displays the originating telephone number of an incoming call, allowing the recipient to know, before answering the call, the number of the party calling.

For law enforcement, caller ID has proven to be a valuable intelligence tool. When investigators install a court-authorized wiretap or dialed number recorder on a telephone line, for instance, they also generally request caller ID. With caller ID on the line, investigators not only know whom the targeted subject calls but also who calls the subject.

Investigators also can include a suspect's caller ID device on a search warrant request. A properly worded search warrant allows investigators to seize the caller ID box and thus obtain an accurate record of the last 25 to 100 calls received by the subject.

Nevertheless, despite its benefits, caller ID poses some potentially serious problems for the police. Critics claim that it invades citizens' privacy. There are also concerns that caller ID may reduce the number of calls to police crime tip lines, crisis centers, and suicide and abuse hotlines. For law enforcement agencies, concerns primarily revolve around the effects caller ID and related services have on undercover operations. By understanding the functions of these services, however, investigators can develop strategies to maintain telephone security during investigations.

The Mechanisms of Caller ID

Caller ID comes in two forms. Basic caller ID (sometimes referred to as single message) represents the first generation of caller identification services, widely available since the early 1980s. During the last several years, telephone companies have been converting to enhanced caller ID (also known as deluxe or multimessage).

The primary difference between the two systems is the amount of information provided about the originating telephone call. While basic service provides only the caller's telephone number and the date and time of the call, enhanced service supplies this information, as well as the name and in some cases, the address of the caller.

Regardless of which form of caller ID serves a particular locality, the mechanics of its operation remain the same. The local tele-

phone company attaches caller ID at its central office after the originating call has been placed. This makes it nearly impossible for the caller to trick or defeat the system.

Once the caller ID codes have been attached, the caller's identifying information is routed on the line with the call itself to the destination telephone. Caller ID information reaches the receiving telephone between the first and second rings. If a call is answered before or during caller ID delivery, the answering party will not receive the data.

Call Blocking

If a caller has installed call blocking—an optional service to prevent transmission of the originating telephone number and other identifying information—this request is attached at the central telephone office after the commands for caller ID have been attached. When the call reaches the central office for the area serving the destination telephone, the office handles caller ID according to local programming. If the party at the destination telephone has paid for caller ID services, identifying information from the originating call will be sent.

If a call blocking command has been attached by the party making the call, the call will go through but the identifying information will not be relayed. Instead, a message indicating that all identifying information has been blocked will accompany the call. Generally, the word "private" or some variation appears on the caller ID screen, notifying the recipient that the caller has concealed the originating telephone number.

Availability

Newly relaxed regulations and advances in technology soon will make caller ID and related services available on a much larger scale. Until recently, regional telephone companies dictated local service availability. Often, parties with caller ID would receive an "out of area" message, indicating that an incoming call was being placed from a locality that did not relay caller identification information.

In December 1995, the Federal Communications Commission allowed caller ID services to be relayed nationwide. As telephone companies gradually expand service availability, caller ID will become a truly national system. Already, there are indications that caller ID will be offered on a worldwide basis in the not-too-distant future.

Rapidly advancing technology also has enabled carriers to offer caller ID services on calls originating from sources that were once immune, including cellular and pay telephones. As with calls from localities that do not pass caller ID, calls from these types of telephones previously would relay an "out of area" message. Now, calls placed from cellular or pay telephones, as well as long-distance calls paid for via credit or phone cards, may provide identifying information to the party being called.

In fact, some firms that specialize in emerging technologies heavily promote their caller identification capabilities. The newest competition to cellular service, personal communications systems (PCS), pass identifying information in both directions. A screen on the handset lets users know the originating telephone number of the party calling them. Likewise, callers using PCS will pass on their identifying information to anyone with a PCS unit or caller ID. PCS users do not need to activate caller ID service separately; the caller identification features are included in the basic service contract.

With expanding caller identification services, law enforcement agencies should study the various methods available to respond to the threats posed to undercover investigations. Because no single antidote exists for every situation, investigators should be aware of the broad range of possible countermeasures to caller ID.

Countermeasures to Caller ID

Given the dramatic growth of caller ID and the impracticality of determining whether an individual has this service option before a call is placed, investigators should assume every subject can identify them when they call. Although caller ID cannot be defeated after a call is placed, investigators can minimize its effects.

Call Blocking

While placing call blocking on the originating telephone line may be the most obvious countermeasure, certain features of this service make it less than practical for undercover operations. As discussed, a message will alert the party on the receiving end that the caller has placed a block on the outgoing line. Such a signal could further inflame the suspicions of an already wary subject.

Then, because call block commands are attached to a call after the caller ID commands, investigators must gamble that the commands—sometimes routed by two different telephone companies—are attached properly. If not, a call from the police station

could be routed unblocked to a subject. While such mishaps are extremely rare, just one could prove disastrous. In response to widespread concerns about privacy issues surrounding caller ID, telephone companies have developed more specialized call blocking features. Per-call blocking defeats delivery of caller ID on a call-by-call basis; per-line blocking defeats caller ID on a specific outgoing telephone line.

In most areas where these features have been introduced, however, the local telephone carrier also offers service options to counter call blocking. The anonymous call rejection feature automatically routes calls with call blocking to a recording that advises callers to dial again without blocking caller ID.

Some state and local governments have arranged with telephone companies to provide call blocking features only for government lines. Still, whether in a general form or on a per-call or per-line basis, call blocking might not provide the stealth necessary for undercover operations. If, however, a law enforcement agency decides to use call blocking in any of its forms, investigators must be careful to ensure that it is attached properly. In some areas, telephone companies use the same code to block caller ID as they do to cancel the block. This can become an especially confusing issue with per-line blocking. When investigators enter the blocking code on a particular line, the end result actually may be to reactivate caller ID on a line where it previously had been blocked. To avoid such scenarios, investigators should not rely on call blocking.

Credit or Phone Cards

While placing calls using a credit or phone card has, in the past, been a fairly safe way to defeat caller ID, investigators cannot assume that these tactics will continue to work every time. An increasing number of telephone companies have begun to relay some type of identifying information via calls placed with credit and phone cards. Telephone companies also may periodically test new features, intermittently relaying identifying information on a limited number of calls before fully engaging a system.

It is increasingly dangerous for investigators to assume that a credit or phone card call will not betray their identities to parties with caller ID. Recent reports indicate that some calls routed by a particular carrier would display "U.S. Government" when placed with a government credit card. Revelations of this type pose obvious dangers both to investigations and investigators.

Pay Telephones

Investigators should remember the limitations of using pay telephones to defeat caller ID. Today, most pay phones relay caller ID information. Industrious subjects can use databases (available to the public) that show the location of each pay phone in a given city to pinpoint a caller's location. One investigator described a case where he called a subject from a pay telephone. While they were still talking, the subject tracked the investigator's position and went to the phone booth shortly after the call.

Investigators should be aware that although a call placed from a pay telephone will not show the caller's name and address, it may show the caller's location. A call placed from a phone booth outside the police station or federal building may be just as disruptive to a case as a call placed from the office telephone.

Undercover Lines

Agencies can use telephone lines dedicated solely to undercover operations. However, regardless of what name is on file, the telephone company will maintain a record of the physical location of the telephone. To enhance security, agency administrators should work with telephone company officials to ensure that the billing address does not reflect a law enforcement connection. The computer containing the wiring information still will connect to the actual location of the telephone, no matter where the bill is sent.

Call Diverters

A device called a call diverter represents one of the more effective countermeasures to caller ID. These devices forward outgoing calls from one telephone line to another, effectively masking the identity of the original caller. By enabling agencies to forward calls at the source, these devices offer more security than call forwarding and other services available from the telephone company.

Units cost between $400 and $5,000, depending on the features included, but may prove well worth the investment for agencies that engage regularly in undercover operations. Investigators should be able to obtain detailed information about call diverters from their agency's electronic surveillance support unit.

Testing Caller ID Availability

Regardless of what technical countermeasure investigators employ to defeat caller ID, they should periodically make test calls from

the telephone they normally use for undercover operations to monitor how caller ID is being handled in a particular area. By calling a telephone equipped with caller ID, investigators can determine what type of identifying information is being relayed via the telephone lines. Calling the local telephone company is not a good indicator; customer service representatives do not always know what specific information is relayed at any given time because, among other reasons, technicians frequently activate new features for testing purposes. However, even conducting regular tests does not ensure security because a subject may have different caller ID capabilities than the investigator's test line.

Automatic Number Identification

Like much of the general population, many investigators might be unfamiliar with automatic number identification (ANI). Intended for use primarily by businesses, ANI provides subscribers with a wealth of identifying information concerning callers. As is the case with caller ID, this service option poses potential security problems for investigators.

Despite its obscurity, ANI actually predates caller ID. The systems serve similar purposes, but unlike caller ID, ANI coding is sent on a separate wire, rather than with the call itself. ANI is available only on numbers beginning with either 800, 888, 900, or 911 or a 976 exchange. Businesses routinely use ANI to gather information on their callers for billing purposes. There is no way to block ANI delivery.

In the wrong hands, ANI can provide criminals with personal information about anyone placing a call to them. During a recent case, a law enforcement officer used an 800 number to access a subject's personal pager. The officer punched in a telephone number different from the one he was calling from for the subject to call. But, because the subject's pager service tracked ANI data and forwarded it to subscribers, the subject was able to tell the officer the number of the telephone from which he originally called.

Because telephone companies do not offer services to counteract ANI, law enforcement agencies must rely on alternate methods to safeguard security. While call diverters represent the most effective countermeasure against ANI, given their cost and impracticality for use during many fast-paced investigative scenarios, investigators cannot rely on them to ensure security for every situation.

Conclusion

While it might be easy to take the telephone for granted, law enforcement agencies cannot afford to become complacent about telephone security. Evolving caller ID services represent a potentially serious threat to undercover operations for law enforcement agencies in an increasing number of communities around the country.

By developing a flexible array of countermeasures, agencies can minimize the dangers posed by caller ID. Investigators must remember that no countermeasure can be guaranteed effective for every situation. Instead, they should take precautions and be prepared for any problem that might arise from breaches of security due to caller ID. After all, the security of law enforcement operations is on the line.

APPENDIX V

NSA Related Information

Note: Since 1993, when I began compiling the information for this book, I have been in touch with former high-level technical consultants who have worked in both the telephone industry and the intelligence community. They confirm that the basic bugging technologies described in this work as either in place and operational, being installed, or being readied for installation. In the meantime, another acquaintance of mine, a former CIA agent, claims that FEMA has set up what it calls its Financial Crimes Enforcement Network of supercomputers designed to track every financial transaction of every citizen. This claim had been made elsewhere, as well. The ability to access valuable information freely and instantaneously is high on the list of priorities of certain elements within government.

The Information Superhighway vs. Constitutional Civil Rights

Bill Clinton's Information Superhighway—really the supposed product and brainchild of the entire communications industry—is being proclaimed as the panacea for today's information and communications overload, and the tool by which the future will be wrenched into today. Upon us is the wonder of being able to reach anyone, anywhere, at any time, and access or share any kind of information—written documents, live or recorded audio and/or video, or even computer programs or files. That kind of informa-

tional access can only leverage the power of business to conduct business faster and with more profitably, magnify our children's educational opportunities and prowess with unlimited potential, amplify our personal entertainment experiences with fantastic new options, and simplify our daily lives with unheralded conveniences and illuminations. But at what price?

The technology that brings these miracles will undoubtedly improve the life and commerce in our nation. But it also has the power to destroy the very foundation upon which America was built. While businesses can use it as a tool for greater success, that tool is a double-edged sword, allowing favored businesses and power brokers to access otherwise unauthorized information and grotesque profit, and giving them the means to mercilessly destroy the competition. While our children might use the Web to learn by leaps and bounds, that which they learn may be insidiously wrong, tainted with viewpoints and thinking biased towards political ends—brainwashing at its best, on those who haven't yet formed a point of view. While we might use the Internet to playfully explore alternate realities, it might be defining for us a new, dark reality where the distraction itself is a tool that keeps us unaware of other matters. While can be used it to improve our daily lives, it may very well be destroying the precious things we value in life in ways we cannot fathom.

This gloomy view, proposed as a cautionary counterpoint to the widely acclaimed and promoted Information Superhighway, is offered for good reason. There are clear indicators of dark intentions by dark forces—unseen forces behind the development and implementation of the Superhighway. The ability to control, restrict, modify, access, and monitor all information is a priceless commodity. Simply put, control of information can mean influence or outright control of any and every aspect of social infrastructure and, thereby, of the actions and thinking of any person or group that accesses that information. The information superhighway has that potential—built in by design. Though highly illegal and morally abhorrent, it offers the potential to sway information pathways with easy and undetectable control, the potential to introduce strategic disinformation, the potential to ultimately control virtually everything and everyone—even to know where they are and what they are doing at all times, on demand.

Obviously, if such control was technically feasible, it would be a tempting goal for any sinister group—and a properly feared sit-

uation for everyone else. The next questions should rightly be: Is it a genuine and reasonable concern? Is it be technically, and practically, possible? If so, who has both the motivation and the wherewithal to achieve such a goal?

Let's take a look at who the key players are—the ones visible publicly: the President and his administration—the information superhighway concept was officially "introduced" by Bill Clinton; the Media—almost immediately a wealth of technical information was offered up in the media, almost as if an organized PR campaign had been planned and executed, with a simultaneous blizzard of "what if" advertisements by AT&T and cable TV companies; and The Military-Industrial-Intelligence Complex (MIIC). Each of these players should be examined closely, their roles scrutinized. Here, we need not separately look at the MIIC because (and this may not surprise anyone) to look at any of the players IS to look at the MIIC.

First of all, let's discuss the President. Without an attempt at full explanation of relevance or providing concrete proof, at least at the moment, let us preface this discussion with a few tidbits of information gleaned from national publications. First, Bill and Hillary Clinton have been accused publicly of being CIA operatives by the *Spotlight*, a weekly, right-wing newspaper that has broken more spy and intrigue stories than any other paper. That the mainstream media has not covered this revelation is no surprise to anyone who has watched the relationship between the CIA and media over the years. At the least, a strong case can be made for a "close working relationship"—all the way back to Mena, Arkansas, a CIA drug-importing/gun-exporting haven during the Governor Clinton/Iran-Contra heyday. That neither the White House nor the CIA have challenged these claims would also be no surprise to CIA watchers—the CIA never acknowledges, challenges, or admits to any charges against it unless directly asked by those empowered to demand an answer, such as the President or Congress. It should also be noted that CIA husband/wife teams are relatively common, typically representing marriages of convenience for all concerned. Howard and Dorothy Hunt, of Watergate fame, is one example of this.

Second, one of Bill Clinton's first acts upon entering the White House was to sign into law a bill which requires manufacturers of common communications devices such as telephones, fax machines, modems, and so forth to incorporate a certain new technology, a specially designed microchip with a unique purpose. That purpose is

to allow government to easily eavesdrop on otherwise secure communications. Of course, the law included "stringent" requirements that the government have duly authorized court orders before proceeding. This revolved around a complex distribution requirement for two portions of necessary encryption information, called "keys," supposedly maintained exclusively in protective custody of two different agencies and released only by the court order. What it did not include was anything to address the fact that almost any key agency of national government with a large enough computer (or perhaps even major corporations and institutions) could locate the codes with clever software and throw the "switch" remotely without having to go through any agency or third party. For that matter, one key intelligence agency, the NSA, the creator of the system, already knows both halves of the equation....

For these reasons, with regard to Clinton's administration, we should also take a look at both the CIA and the NSA—the top two intelligence entities responsible to the President. From firsthand knowledge I gained while investigating illegal domestic spying by CIA elements upon American citizens, local government, and business, two interesting things have surfaced. As far as the CIA is concerned, there is growing evidence that "rogue" fronts—seemingly innocent electrical-contracting companies specializing in serving local government and the high-tech industry—are systematically spying on their clients and other targets. I make these charges based on the fact that such an electrical contractor spied on me. My subsequent investigations of them included my observation of their operatives entering otherwise technically secure areas of major high-tech firms after hours—easily bypassing alarm systems and going about their business without any company representatives around. Armed with both technical ability and complete access, it appears the CIA has established a network of such firms nationwide—at the very least, they are well established throughout five northwest states, with hundreds of locations. Everything about their background points to CIA affiliation.

Clipper/Chipper

For the NSA, which fosters a nest of spies many times larger and more secretive than the CIA, there are very interesting recent developments. I have worked for a company that sold special software to the NSA, software used in signal-processing projects in the communications arena, and have had discussions with an unusual-

ly talkative the NSA researcher regarding development of specialized communications chips for the NSA. The information I gleaned from these encounters, which has subsequently been confirmed by articles in assorted national publications and local newspapers, regards NSA development of two specialized microchips, code-named Clipper and Chipper.

Chipper is apparently a specialized data capture and decoding chip. Clipper is Chipper's counterpart, a specialized data encoding chip containing a built-in "back door." In the world of digital devices, a back door is a secret electronic entrance into a digital information system. Simply put, Clipper can, upon remote command by Chipper, provide instant access to decoded information processed by any device with Clipper installed. If the data stream is encrypted by the sender, the Clipper/Chipper pair instantly decodes it on the fly, since the usual means of encryption will be provided in hardware by the sending device itself, for which Clipper already knows the decryption key. All other commercial encryption methods can be decoded handily by NSA computers, for all encryption algorithms and devices must, by law, meet restrictive NSA requirements. Anyone using illegal encryption schemes may or may not slow NSA decryption, but they most certainly run the risk of stiff fines and imprisonment. In accordance with the communications bill signed by Clinton, all digital communications devices manufactured must include Clipper chips within the design. Actually, Clipper circuitry will likely be covertly included within standard communications chip designs, and most manufacturers will not even be aware of the installation. They will simply be using parts which fit government specifications for communications devices. Even chip manufacturers may be largely unaware.

Similarly, there have been like inroads made in the telecommunications and cellular-communications industries. The key is the conversion of all traditional systems to the new digital systems. In the act of converting an analog signal, such as in a telephone call, into a digital signal before transmission, it becomes a simple matter to piggyback additional information onto the original signal without detection. This added information can include data about the caller or the person receiving the call, specifications regarding the equipment being used or its location, encryption decoding specifications, or even commands to digital versions of tape recorders or other sophisticated listening devices or telephone switching systems. Encoding can be a 2-way function, which can

further provide for telling the caller or callee's systems to execute functions that neither party would approve of willingly, such as activation of the handset's microphone even when the phone is on the hook and not in use.

The NSA has been working with telecommunications equipment manufacturers to create an extensive network of remotely programmable system monitors to manage what might otherwise seem impossible—the electronic bugging of and illegal eavesdropping on an entire nation. Central to this scheme are components in the digital telephone system—where calls from individual area telephones are fed into units designed to collect and convert calls to digital signals, and distribute them en masse via fiber-optic bundles towards their destinations. These "connection nodes" have been designed to automatically detect and implement special programming instructions embedded within the data streams carrying the audio information of telephone calls. Thus, each node can be programmed by the telephone company to properly handle any change in caller service or even compensate for equipment failures elsewhere. Unfortunately, anyone who knows the programming requirements and has a fast enough computer can access and apply this technique for any purpose. The future is a 100 percent digital system, from your phone to the government's computer banks.

For the telephone company and their clients, the technology provides superior service, quality, reliability and capability. However, it also provides the NSA and other government agencies with additional new capabilities of a more sinister nature. Since these devices simply look for the special programming instructions, which are transmitted in a special, high-speed data packet, any properly constructed data packet containing instructions will be executed—regardless of who sent them. The nodes cannot tell where instructions come from, they simply obey. Calls and call information can be rerouted, captured, and decoded at will by anyone with the ability to send the correct data packets to the correct node. The telephone companies are the only ones authorized to do so, and since specialized, high-speed supercomputers are required to implement these functions, the idea that this is an appropriate defense against invasion of privacy seems sound. Yet the illusion is shattered by the fact that the NSA helped to develop the very technology used here, and the agency has the same supercomputers at its disposal. And many of its intelligence-community partners enjoy the same abilities.

By the use of NSA supercomputers, and with a simple computer-generated phone call, nodes can be told to take specific actions on specific calls to or from a given number, select groups of numbers, or even whole areas served by the target node. Calls can then be rerouted to pass through the NSA supercomputer, associated filters, or any other desired destination. They can be recorded digitally and use real-time processing to look for key words, names, number sequences, or recognizable voice patterns (useful in tracking individuals). Matches can be filed and indexed, reports compiled, and notice provided to agents for review and follow-up action. Calls can also be derailed (allowing agents to answer, pretending to be the correct party) or simply rerouted to a perpetual busy signal, or they can be routed to a more traditional manned listening post. Versions of this concept, which are advertised as "helpful" features for the caller, have already been implemented in cellular communications systems. The system is already in place and is steadily being expanded.

Lest some doubt these accusations because they seem too fantastic, questioning either the technological feasibility or the extent of a "Big Brother," it might be wise to consider what the NSA has already done. One might recall the embarrassing private phone calls between Princess Diana of Wales and her lover, calls which found their way into the press. According to a piece that aired on *60 Minutes*, the source of the "leak" was an NSA monitoring station located in Great Britain. This station was designed to monitor all radio and cellular communications there (presumably as a service to MI-5, the British secret service, and the CIA). Using supercomputers, the NSA could record phone calls and sift through them to catch key words or phrases. Sound familiar?

David Burnham, in *The Rise of the Computer State*, has a whole chapter devoted to fears of Big Brother's mainframes. The NSA, which is the largest U.S. intelligence agency and one not subject to any oversight, is described as having the world's best computers. It quotes 1970's Senate Intelligence Committee head, Frank Church, as warning that "if not properly controlled, [NSA's technological capabilities] could be turned against the American people at a great cost to liberty." Also cited is the 30 years' worth of NSA operations to intercept copies of virtually all telex messages to and from the United States. It also alleges that the CIA illegally intercepted thousands of first-class letters leaving the country. Church concluded that, if the NSA's technological abilities were turned

against Americans, "No American would have any privacy left.... There would be no place to hide."

The NSA and Corporations

Another interesting NSA involvement can be found in FCC and FTC actions that have wholeheartedly embraced corporate megamergers and sweeping changes in the communications industry. Close scrutiny of each such merger or change, going back to the dissolution of Ma Bell into "Baby Bells," reveals that each has provided significant benefits to the corporations, well beyond the benefits publicized as being for the consumer. Furthermore, as those who watch and track CIA proprietaries and key "former" CIA managers who join private enterprise can attest, there is an amazing pattern of CIA and intelligence-community involvement with corporations. Indeed, many such companies frequently provide discreet services to the intelligence community upon request—enjoying a close relationship which benefits both parties. Some high-tech firms even consider themselves to be branches or extensions of the federal government, according to some intelligence insiders, and at least two major computer makers admit to building in back-door access to allow quiet government access (presumably for reasons of "national security"). Dozens of books on the intelligence community have highlighted many of these relationships, and many news stories document others. Collectively, these "coincidental" events become staging moves for Information superhighway and the darker possibilities of its manipulation.

The Media

Let us now take a quick look at the media—defined here as mainstream broadcast and print resources. This includes the major networks, cable news producers, major newspapers and major national publications. As has been reported time and again by media watchdogs such as Noam Chomsky and Ben Bagdikian , there are very few entities (less than 30) that own and control the many hundreds of mainstream news outlets, and even among the few owners, there is a kind of forced interdependency and common sharing of resources. Most daily newspapers have become mere news-clipping agencies dependent on the same two or three wire services that everyone else uses for their news—including at least one "former" CIA proprietary. This means that a handful of people write the news that everyone reads. In general, by hiring editors of

similar thinking, even editorial policies and news slants will tend to favor those of the megamedia corporate owners, at least when it comes to the important issues—that is, those they deem important, not necessarily the same ones we think important.

What is bothersome about this is that the corporate entities that govern the mainstream media, including the wire services, can be shown to have direct links to CIA. These have been chronicled in several books and other publications on the intelligence community, and even some covering media itself. If this were not enough, almost all of the key players in media, communications, and government all share memberships in those same troublesome "one world" groups: the Council on Foreign Relations, the Bilderbergers, and the Trilateralists. Almost any casual study of these groups, and the criticisms against them, would be enough to raise suspicion.

One might ask how many coincidences it takes before one sees a conspiracy. The conspiracy exists; what we must do now is look to see where it is headed and fight it. The end result of a successful conspiracy is absolute political and financial control of our nation, of the world. The conspirators are seeking to remake the world into a single, united corporate state. Welcome to the Information Superhighway.

I would be interested in purchasing old catalogs, training materials, and technical documentation used by Audio Intelligence Devices, HDS, and other surveillance companies. Specifically, I am looking for old product catalogs, sales materials from trade shows (such as NATIA), training manuals, textbooks from the National Intelligence Academy, product owner's manuals, and product service manuals.

Mr. Atkinson is especially interested in purchasing whole "generations" of materials, so if you have, say, ten years' worth of old catalogs from the 70s, don't discard it. You can reach me by e-mail through my Web site, at www.proparanoid.com to discover if what you have is of interest and to work out payment.

Understand the Mr. Atkinson is interested in the actual items for practical reasons (being in the business of training TSCM operators), where as I am more interested in documenting their existence and application for posterity's sake. Thus I would appreciate being the contact on any such resources. This interest does not extend to any materials which may be deemed officially "classified" as secret or sensitive, or which may be potentially damaging to

general national security interests—except where such may reveal criminal acts in the guise of "national security." As an author, I can and do legally protect my sources.

I hope to provide ongoing resources for anyone who is in true need of help. For that reason, I am establishing a subscription newsletter for readers of *The Professional Paranoid* and others who may otherwise be aware and in need. The emphasis of the newsletter will be to continually update readers about what does and does not work in particular situations—new ideas and techniques for specific problems, especially those which may not have been addressed directly within *The Professional Paranoid.*

Anyone may submit problematic "situations" for review and tactical advice. The newsletter will also provide news on what's new in the "trade" of security, surveillance, and countermeasures. Anyone submitting information for possible inclusion or review in the newsletter should read and follow the guidelines provided below.

The newsletter will be published quarterly. Subscription will be $15 a year by mail, or $10 for e-mail distribution, subject to change without notice. To subscribe, send a check or money order made out to The Professional Paranoid. The address for payments has not been determined as of the date of publishing, but will be available at the author's Web site by the time the book is in distribution. Please visit www.proparanoid.com to obtain the address, or contact Feral House (ask their catalog while you're at it!). If you do not have a computer or Internet access, consider visiting the public library. Many libraries offer free Internet access and help in getting online.

If submitting material for review or inclusion in the newsletter, please follow these guidelines:

1. Do not send or reveal anything sensitive or confidential. Speak in generics, rather than specifics. Use substitute and fictitious names if needing to refer to individuals, well-known places, businesses, etc. If your situation/information is referenced in the newsletter, even your name will be fictionalized for your protection.
2. Keep the background brief: try to keep it to one paragraph to describe yourself and your resources (financial, allies, employment, state of security, etc.); one paragraph to generically describe your enemy (if known) and their resources; one para-

graph to describe the apparent basis or motive behind your problem; one paragraph each to describe various tactics tried and their results.

3. If looking for help, provide a basic set of specific questions you wish me to address—and tell me what you think each answer should be, and why. If trying to advise of a particular trick or technique that worked well, go into as much detail as you find appropriate.
4. Provide a means of e-mail or mailed response which you consider safe from prying eyes. An attempt will be made to respond within 72 hours of e-mail requests or within fifteen days of mailed requests. I cannot respond by telephone unless you wish to accept the charges and unless you are very specific about good times and dates to call.

APPENDIX VI
Useful Internet Search Sources

Multi-engine Websearch:
http://www.dogpile.com/

Dogpile uses the following search mechanisms, and all at once:

The Web: Yahoo!, Lycos' A2Z, Excite Guide, GoTo.com, PlanetSearch, Thunderstone, What U Seek, Magellan, Lycos, WebCrawler, InfoSeek, Excite & AltaVista.

Usenet: Reference, Dejanews, AltaVista and Dejanews' old Database.

FTP: Filez and FAST FTP Search.

News Wires: Africa News , Agence France , M2 Airlines, Asiainfo, Business Wire, Canadian Corp, Content Factory, Fednet, Infolatina, InterPress, Interactive Sports, Itar-Tass, M2, Phillips, PR News, PIO, Resource News, SABI, UPI, US Newswire, Washington Tech, WENN, Xinhua, Yahoo News Headlines, Excite News and Infoseek NewsWires.

Usenet/Newsgroups Search Engine:
http://www.dejanews.com/

Mailing List/Discussion Group Search Engine:
http://www.liszt.com/intro.html

Guide to Internet Info Resources (Argus Clearinghouse):
http://www.clearinghouse.net/

People / Phone Searches:
http://www.inlink.com/~nomi/vitaife This page contains information about where to obtain vital records from each state, territory and county of the United States.
http://www.primenet.com/~hamrick/names/ Enter a surname (last name) into the form in this site and you'll get a map of the United States showing the distribution of people with this surname within the 50 states.

The source of this data is the 1850 Census, 1880 Census, 1920 Census, and 1990's phone books.

Social Security Death Index:
http://www.ancestry.com/ssdi/advanced.htm

Social Security Number Lookup
http://www.informus.com/ssnlkup.html What Can A Social Security Number Tell You?

Military Locator Service:
http://www.militarycity.com/

Adoptees Search Network:
http://www.idir.net/~pbrown/ For location of specific names.

BirthQuest Works.
http://www.access.digex.net/~vqi/top.html Online searchable database dedicated to searching Adoptees, Birth Parents, Adoptive Parents and Siblings.

Adoptee Search Group
http://www.adopting.org/adoptees.html For adoptees trying to find foster family or birth relative.

Gopher to find email addresses:
gopher://gopher.tc.umn.edu

Telephone Directories:
http://www.uiuc.edu/cgi-bin/ph/lookup

http://www.infospaceinc.com/
http://people.yahoo.com/
http://www.switchboard.com/
http://www.555-1212.com/aclookup.html (area code directory)
http://www.payphones.com/ (list of pay phone providers nationally)
http://www.lcweb.loc.gov/cgi-bin/phf/ (Library of Congress employee directory)
http://www.pagenet.net/pagenet/page_inp.htm (sends Pagenet brand pager messages)
http://www.uswest.com/directorysource/index.html (telephone directories for sale, including business guides, electronic directories, cross-reference and city directories, import-export directories, fax directories, SIC directories, ZIP code directories, 800 number directories)
http://yellowpage.net/search.asp
http://s12.bigyellow.com/ (American Yellow Page directories)
http://www.superpages.com/ (American and Canadian Yellow Pages directory.)
http://www.worldyellowpages.com/ (international business directory)
http://www.att.net/find/ (White Pages, Yellow Pages, maps, student directories, colleges, universities, government workers, international directories, genealogy, classified ads.)
http://www.whowhere.lycos.com/ (web people finder)
http://worldemail.com/wede4.shtml (The World Email Directory is an online Internet database search engine. Retrieve information even if you have only a partial email-address, zipcode, or partial telephone number. Combined Personal Directory, Phone and Fax Directory, Business Directory, Yellow Pages, White Pages, Zip Code Directory, Email Directory, and Homepage Directory all in one.)

Address Site:

http://www.cedar.buffalo.edu/adserv.html Given a U.S. postal address, this server attempts to rewrite the address in the proper format along with the ZIP+4 code. If it is successful, you can retrieve a Postscript or a GIF file of the address for printing, with a barcode! You can also view a street map of the address, from two different Internet map sites (MapBlast and MapQuest).

Maps Interstate Highways East of the Mississippi River:
http://interstatelink.com/isl/ius.html

Missing and Exploited Children Listings Sites:
http://www.missingkids.org/
http://www.childquest.org/

Death and birth date tracing
http://kadima.com/ (Database consists of over 200 million names, 170 million with date of birth compiled from multiple public, private, and proprietary sources.)

For a fee, screens credit and criminal reports and background refs:
http://www.informus.com/

Legal Directories

Legal Information Sites:
http://law.gsu.edu/library/LibraryResources/InfoSeries/General/LegalInfoOnWeb.htm
http://www.wwlia.org/us-home.htm (Includes a good legal dictionary, making plain English of arcane legal terms.)

Law Net Forum:
http://law.net/ (Post questions and answers about any legal matter or list job opportunities in the legal community — whether seeking professional legal opinion, or you are an attorney looking to exchange information with others in your area of expertise.)

Federal and State Courts Finder:
http://www.law.emory.edu/FEDCTS/

Supreme Court Opinions:
http://fedbbs.access.gpo.gov/court01.htm

State and City Law Listings:
http://seamless.com/road.html (1. Consumer Law and Commercial Class Action 2.Criminal Law 3. Information Law & Intellectual Property 4. International Law 5. Insurance Law 6. Misc. Links 7.Politics & Washington.)

United States Code:
http://law.house.gov/ (Full text searchable copy of the United States Code and acccess to the other law resources of the Internet.)

Law Source Material:
http://www.law.cornell.edu/topical.html (Law of Commercial Transactions, Enterprise Law, Law Relating to Particular Activities or Business Sectors, Law Relating to .Property, Natural Resources, the Environment. Intellectual Property, Taxation, Constitutional Law, Individual Rights, Family Law, Employment Law, Accident and Injury Compensation and Prevention, Criminal Law and Criminal Procedure, Courts, Court Procedure, Evidence, Remedies, and Alternatives, Governmental Organization, Power, and Procedure, Public Benefits, Health and Human Services, Practice of Law, Legal Education, Legal Theory, International, Transnational, Comparative Law.)

State Statutes:
http://www.law.cornell.edu/topics/state_statutes.html

Books/Written Material

Virtual Library Sources:
http://www.elibrary.com (Full-text newspapers and magazines, national and international news wires, 2,000 complete works of literature, Over 28,000 photos, images and maps, television, radio and government transcripts.)

Links to Virtual Libraries:
http://coombs.anu.edu.au/ResFacilities/DemographyPage.html

Published and out-of-print books:
http://lcweb.loc.gov/catalog/ (Library of Congress site also includes gateway for searches through more than one hundred academic library catalogues.)

Library Catalogues:
http://www.lights.com/webcats/
gopher://libgopher.yale.edu
(Both domestic and international.)

Medical Journal Searches:
http://www.healthy.net/Library/search/medline.htm

Most commonly prescribed drugs by brand name, generic name, indications and contraindications:
http://www.rxlist.com

Government Searches

Government Documents:
http://www.access.gpo.gov/su_docs/dbsearch.html
(Budget of the United States Government, Catalog of U.S. Government Publications (MOCAT), Code of Federal Regulations, Commerce Business Daily, Congressional Bills, Congressional Directory, Congressional Documents, Congressional Hearings Congressional Record, Congressional Record Index, Congressional Reports, Economic Indicators, History of Bills, Miscellaneous House Publications, Miscellaneous Senate Publications, Public Laws, Federal Register, GAO Comptroller General Decisions, GAO Reports, Government Information Locator Service (GILS) Records, Privacy Act Notices, Sales Product Catalog (SPC), Supreme Court Decisions, U.S. Government Manual, Weekly Compilation of Presidential Documents.)

Census Data:
http://www.census.gov/

County and City Data Books:
http://fisher.lib.Virginia.EDU/ccdb/
(Provides WWW access to the electronic versions of the 1988 and 1994 County and City.)

Reporting Government Fraud:
http://www.gao.gov/fraudnet/fraudnet.htm

National Archives and Records Administration
http://www.nara.gov/ (Contains the following databases: NARA Archival Information Locator [NAIL], John F. Kennedy Assassination Records Collection, Guide to Federal Records in the National Archives of the United States Government Information Locator Service [GILS].)

CIA Home Page
http://www.cia.gov/cia/ciahome.html (Includes a heart-warming "homepage for kids.")

Declassified Government Papers
http://www.parascope.com/dossier.htm (Offers hundreds of declassified government documents and analysis of covert ops and propaganda campaigns worldwide.)

NASA Home Page
http://www.nsa.gov:8080/

"Your FBI" home page:
http://www.fbi.gov/

Full Disclosure / How to Obtain FBI Records
http://www.glr.com/fbi.html

Thousands of FBI files secured by FOIA:
http://www.crunch.com/01secret/01secret.htm

SEC records here:
http://www.sec.gov/cgi-bin/srch-edgar

Patent, Trademark and Copyright searches
http://www.lapl.org/central/intellec.html#searchtips

Center for Disease Control and National Center for Health Statistics:
http://wonder.cdc.gov/
http://www.cdc.gov/nchswww/default.htm

PANNA's [Pesticide Action Network North America] search site:
gopher://gopher.igc.apc.org/11/orgs/panna/pestis

Environment-Watch Websites:
http://www.envirosearch.com/search.htm

RTK Net:
http://rtk.net/ (Provides free access to numerous databases, text files, and conferences on the environment, housing, and sustainable development.)

Who gave What to Which Federal Candidates:
http://www.tray.com/fecinfo/

Disasters, Natural or Otherwise:
http://ltpwww.gsfc.nasa.gov/ndrd/

Private Investigation Sites

Private Investigations Site:
http://www.pi-mart.com/

Information and equipment for telephone bugging:
http://www.tscm.com/

Also from Feral House

Psychic Dictatorship in the U.S.A.
Alex Constantine

Bombing minds rather than bodies is the warfare of the new millennium. This book uncovers the terrifying extent of electromagnetic and biotelemetric mind control experimentation on involuntary human subjects.

"The evidence presented in this book is a savage indictment of democracy-turned-dictatorship. The sordid truth about what really goes on in the halls of power is often too much to take, but it does help to have some idea of what we're up against."—*Nexus*

222 pages • illustrated • ISBN 0-922915-28-8 • $12.95

Virtual Government
CIA Mind Control Operations in America
Alex Constantine

Mind Control dwells in a twilit zone of so-called "alien invasions," "zombie killers," "cult murder/suicides," "remote viewing," and "lone nut assassinations." Remarkable researcher Alex Constantine connects the dots on such crimes as cia experiments on children, the infestation of American media by intelligence operatives, mob/drug connection to the murder of Nicole Simpson, and the integration of Nazis into U.S. government operations. "Alex Constantine is the foremost journalist and contemporary historian of the murky worlds of vice and vice-squads."—Donald Freed

301 pages • ISBN 0-922915-45-8 • $14.95

The Octopus
Secret Government and the Death of Danny Casolaro
Kenn Thomas and Jim Keith

Casolaro was murdered by sinister forces as he was researching his unfinished book, *The Octopus*. This volume picks up Casolaro's existing notes, retracing his fatal steps, from investigating stolen police software to bizarre murders in tribal lands to dirty tricks accomplished by the notorious Wackenbush security firm.

181 pages • photos • hardcover • ISBN 0-92215-39-3 • $19.95

To order from Feral House:

Send check or money order, add $3 shipping for first item, $1 each additional item to: **Feral House • 2532 Lincoln Blvd. Suite 359 • Venice, CA 90291**

www.feralhouse.com
send sase for free catalogue

Current Affairs $12.95

THEY'RE OUT THERE. AND THEY COULD BE AFTER YOU.

- Stalkers.
- Corporate Bullies.
- Gangs.
- Professional Criminals.
- The IRS, and a Host of Government "Intelligence" Agencies.

Security expert H. Michael Sweeney tells you how to make sure your suspicions are legitimate, and what you can do about them—how to use and protect yourself against wiretaps, computers and scanners. No less important is the author's explosive info on territorial defense and psychological issues, including mind control.

THE PROFESSIONAL PARANOID picks up where Gavin De Becker's *The Gift of Fear* left off. A necessary read for the unrepentant paranoid in all of us.

"As a defendant in a battle to publish writing deemed dangerous by the government, I have relied upon Sweeney's first-rate guidance, and can vouch for the effectiveness of the techniques he has developed in the trenches and reported in this book with clarity and precision. Those whose nemesis is of a personal nature will also benefit from studying this unique and invaluable resource."—Sondra London, co-author of *The Making of a Serial Killer*

ISBN 0-922915-54-7

51295>

9 780922 915545

FERAL HOUSE

Design by Linda Hayashi